INCIDENTES DE SEGURIDAD EN LAS PASARELAS DE PAGO

Juan David Poveda Gómez
Jorge Iván Salinas Herrera
Luis Felipe Bravo Amaya

Directores:
Ernesto Cadena Muñoz

UNIVERSIDAD SANTO TOMAS
FACULTAD DE INGENIERÍA DE TELECOMUNICACIONES
ESPECIALIZACIÓN EN GESTIÓN DE SERVICIOS DE TECNOLOGÍAS DE LA INFORMACIÓN
BOGOTÁ, 2024

AGRADECIMIENTOS

Agradecemos primeramente a Dios, por darnos los conocimientos, las capacidades, y habilidades necesarias para concluir y desarrollar esta investigación, sin él no sería posible alcanzar cada uno de los objetivos y metas que nos proponemos; así mismo, damos gracias a la docente Ernesto Cadena Muñoz por estar presente en todo este proceso integral de formación; por último, agradecemos a todos nuestros familiares y seres queridos que nos apoyan día tras día y están presentes en nuestra evolución profesional.

Tabla de Contenido

LISTA DE FIGURAS

ACRÓNIMOS

TIC: Tecnologías de la información y la comunicación

TI: Tecnologías de la Información (TI)

IA: Inteligencia artificial

MFA: Multi factor authentication.

DRP: Plan de recuperación ante desastres (Disaster Recovery Plan o DRP).

INTERPOL: Es una abreviación de "international police" (policía internacional).

DIJIN: Dirección de Investigación Criminal e Interpol.

AWS: Amazon Web Services.

CDT: Certificados de Depósito a Término.

CDAT: Certificados de Depósito de Ahorro a Término.

RESUMEN

Este documento destaca la importancia crítica de abordar los desafíos de seguridad presentes en las transacciones en línea, centrándose específicamente en las pasarelas de pago. Se identifican múltiples causas que contribuyen a los incidentes de seguridad, tales como la falta de conocimiento en el manejo de pasarelas de pago, la interceptación de comunicaciones y vulnerabilidades en las plataformas. Estos incidentes, que pueden resultar en la pérdida de activos financieros, datos y confianza de los usuarios en compras en línea, son detallados con sus consecuencias asociadas.

Además, está monografía subraya los esfuerzos regulatorios en América Latina, con énfasis en México y Colombia, dirigidos a mejorar la seguridad en transacciones financieras en línea. El papel clave de las empresas como FinTech, utilizando blockchain para mejorar la seguridad y eficiencia en los servicios financieros y transformar la industria bancaria, también se resalta en este informe. Además de ello se presenta un caso específico en Colombia, donde se informa sobre un preocupante aumento de delitos informáticos, particularmente la suplantación de identidad durante la pandemia.

Por último, en el documento, se propone una solución integral que incluye la educación de los usuarios a través de cursos interactivos y la implementación de códigos CVC dinámicos para entidades financieras. Estas medidas buscan proteger a los usuarios y a las instituciones financieras contra amenazas cibernéticas, asegurando la confidencialidad de los datos financieros en transacciones en línea. Además, se exploran las tendencias del mercado con el objetivo de analizar y establecer la propuesta de valor en torno a la solución presentada en el informe. Este enfoque busca abordar las notables disparidades presentes en los procesos sancionadores, los cuales generan desgastes tanto económicos como psicológicos

en los clientes. Esta situación repercute directamente en la experiencia del usuario, provocando pérdidas económicas significativas. El documento identifica variables relevantes en esta problemática específica y detalla los objetivos concretos que se pretenden alcanzar mediante la implementación de la propuesta sugerida. El análisis exhaustivo de estos aspectos es fundamental para comprender y resolver eficazmente los desafíos que plantea esta situación.

ABSTRACT

This paper highlights the critical importance of addressing the security challenges present in online transactions, specifically focusing on payment gateways. Multiple causes are identified that contribute to security incidents, such as lack of knowledge in the management of payment gateways, the interception of communications and vulnerabilities in the platforms. These incidents, which can result in the loss of financial assets, data and user confidence in online purchases, are detailed with their associated consequences.

Additionally, this monograph highlights regulatory efforts in Latin America, with emphasis on Mexico and Colombia, aimed at improving security in online financial transactions. The key role of FinTech companies, using blockchain to improve security and efficiency in financial services and transform the banking industry, is also highlighted in this report. In addition, a specific case is presented in Colombia, where a worrying increase in computer crimes is reported, particularly identity theft during the pandemic.

Finally, the document proposes a comprehensive solution that includes user education through interactive courses and the implementation of dynamic CVC codes for financial entities. These seek to protect users and financial institutions against cyber threats, ensuring the confidentiality of data measured in online financial transactions. In addition, market trends are explored with the aim of analyzing and establishing the value proposition around the solution presented in the report. This approach seeks to address the notable disparities present in sanctioning processes, which generate both economic and psychological wear on clients. This situation has a direct impact on the user experience, causing significant economic losses. The document identifies relevant variables in this specific problem and details the specific objectives that are intended to be achieved through the implementation of the suggested proposal. The exhaustive analysis of these aspects

is essential to understand and effectively resolve the challenges posed by this situation.

INTRODUCCIÓN

“El ámbito de las transacciones en línea ha sido testigo de un crecimiento exponencial en los últimos años, sin embargo, este avance tecnológico ha traído consigo desafíos significativos en términos de seguridad y protección de datos financieros. En este contexto, la presente propuesta se enfoca en abordar y mitigar los incidentes de seguridad en las pasarelas de pago, con el objetivo de salvaguardar la confianza de los usuarios y reforzar la seguridad en entornos digitales.” [1]

Este documento se organiza para explorar a fondo las soluciones propuestas para reducir los riesgos asociados con las transacciones en línea. Se destaca la necesidad crítica de implementar medidas adicionales de seguridad, dado el crecimiento alarmante de los incidentes de fraude y seguridad informática en el ámbito de las transacciones electrónicas en Colombia.

Se examinan tanto las tecnologías de Amazon Web Services (AWS) como Microsoft Azure como alternativas viables para garantizar la generación segura y confiable de códigos CVC dinámicos, destacando su importancia en la protección de datos financieros y en la prevención de vulnerabilidades.

El presente trabajo identifica el problema de seguridad asociado con las transacciones en línea, así como el enfoque adoptado, detallando las estrategias de implementación técnica y las medidas de respaldo para garantizar la continuidad del servicio. En resumen, este documento proporciona un análisis exhaustivo de las soluciones propuestas para mejorar la seguridad en las pasarelas de pago en línea, subrayando la relevancia y la necesidad crítica de estas medidas en el entorno digital actual.

1. PROBLEMA

“El progresivo avance tecnológico que estamos viviendo, ha traído consigo numerosos beneficios, pero al mismo tiempo ha dejado al descubierto ciertas falencias en los mecanismos de seguridad utilizados en las transacciones en línea, en este nuevo entorno del comercio electrónico.” [2] “Esta problemática de los incidentes de seguridad en las pasarelas de pago, representan un desafío multidimensional que amenaza tanto la seguridad de los usuarios como la integridad de las empresas en línea. También, abarca una serie de causas profundamente arraigadas que están en constante evolución y que, en última instancia, socavan la confianza y la eficacia de nuestras actividades en línea.” [3]

“El reciente Panorama de Amenazas para América Latina revelado por 'Kaspersky', una empresa global de ciberseguridad y privacidad digital mostró que en Colombia se han experimentado 2,4 millones de intentos de 'phishing' durante el 2023, lo que significa en un aumento del 12.5%. Por lo tanto, en promedio ha habido 4 ataques por minuto en todo el territorio nacional, convirtiéndose en el cuarto país más afectado de la región, con un total de 30,9 millones intentos de ataque. El 'phishing' es una modalidad de ciberataque en la que, por medio de correos electrónicos, mensajes de texto, llamadas telefónicas o sitios web fraudulentos, los ciberatacantes buscan que las personas descarguen un malware, compartan información confidencial o realicen otras acciones que los exponga a ellos mismos o a sus organizaciones al ciberdelito. El listado de países más afectados por intentos de ataque de 'phishing' en América Latina es el siguiente, según 'Kaspersky': Brasil con 134 millones de intentos, México con 43 millones de intentos, Perú con 31,5 millones de intentos, Colombia, con 30,9 millones de intentos y Ecuador con 12,2 millones de intentos. Ante esta situación, el phishing continúa siendo el vector más importante para el robo de datos personales y es el primer paso de los ciber incidentes que resultan en fugas de datos masivas.” [4]

“Existen diversas estrategias que utilizan los ciberdelincuentes para el robo de información, una de las más comunes en Colombia es el smishing (el término es una combinación de “SMS” y “phishing”). Es una técnica utilizada por ciberdelincuentes para engañar a las personas a través de mensajes de texto, haciéndose pasar por entidades legítimas, utilizando tácticas persuasivas para engañar a las víctimas con el objetivo de obtener información personal, contraseñas o realizar transacciones fraudulentas. Estos mensajes suelen contener información alarmante, atractiva para incitar a la víctima a tomar medidas impulsivas incluyendo enlaces que dirigen a páginas web falsas o descargan malware en los dispositivos de las víctimas, los atacantes pueden pedir a las víctimas que ingresen información confidencial, como contraseñas o datos bancarios. Por ejemplo, estos mensajes parecen provenir de un banco, solicitando la verificación de la cuenta o la actualización de datos. También, se pueden presentar usualmente como notificaciones de premios o regalos falsos que requieren acciones inmediatas, como proporcionar información personal.” [5]

“El vishing es otro tipo de estafa común en Colombia, que se realiza a través de llamadas telefónicas con el objetivo de obtener los datos personales o bancarios de una persona. Los ciberdelincuentes se hacen pasar por una persona, una empresa, servicio o banco y buscan obtener información privada. A veces engañan diciendo que un conocido se accidentó o está secuestrado. En Colombia es conocido como 'llamada millonaria'.” [6]

“Por otro lado, en el año 2020 Falabella Colombia, fue víctima de un fraude con tarjetas de crédito en el que se robaron los datos de las tarjetas de más de 100.000 clientes. Los ciberdelincuentes utilizaron esta información para realizar compras fraudulentas en línea.” [7]

“Otro ejemplo de ataque cibernético, fue el que sufrió la empresa IFC Networks, proveedora de telecomunicación y que suministra servicios en tecnología afectando a varias entidades del Estado colombiano. El ciberataque mantuvo bloqueado el acceso a las páginas web de la Superintendencia de Industria y Comercio, la Superintendencia de Salud, el Ministerio de Salud y Protección Social y el Consejo Superior de la Judicatura, plataformas que mostraban avisos de error, estado fuera de línea o problemas técnicos al intentar ingresar afectando los canales de atención digital de estas y otras entidades del Estado”. [8]

“El contexto actual de la ciberseguridad en Colombia es complejo y desafiante. En 2023, Colombia sufrió un ciberataque masivo que afectó a más de 20 entidades públicas y 78 privadas, demostrando que el país está experimentando un aumento significativo en la cantidad y sofisticación de este tipo de amenazas.” [9]

“La importancia de la educación en ciberseguridad es fundamental para preparar a las personas y las organizaciones para los ciberataques. Las personas deben estar informadas sobre las amenazas cibernéticas y cómo protegerse, y las organizaciones deben capacitar a sus empleados en ciberseguridad para que puedan identificar y evitar los ciberataques.” [10] “Para protegerse de los ciberataques, se debe desconfiar de mensajes no solicitados especialmente si contienen enlaces o solicitan información personal, verificar la autenticidad confirmando la legitimidad de los mensajes contactando directamente a la entidad a través de canales oficiales, no hacer clic en enlaces dudosos evitando hacer clic en enlaces de mensajes sospechosos y no descargar archivos adjuntos de remitentes desconocidos. Utilizar soluciones de seguridad, mantener actualizado el software de seguridad en dispositivos móviles y considerar el uso de aplicaciones antivirus.” [11]

“Desde otra perspectiva, Evertec considera esenciales las siguientes recomendaciones de seguridad para proteger a los usuarios al realizar pagos en

línea: 1. Elija cuidadosamente el lugar de pago: Los usuarios deben ser selectivos al elegir dónde realizar sus pagos en línea. Aunque las promociones pueden ser atractivas, es importante verificar la autenticidad del sitio antes de proceder. 2. Verifique la conexión segura: Antes de ingresar cualquier información de pago, asegúrese de que el sitio web tenga el icono de "candado" en la parte superior izquierda de la barra de direcciones del navegador, lo que certifica que la conexión es segura y los datos estarán cifrados durante la transmisión. 3. Prefiera e-commerce reconocidos: Realice transacciones en sitios de comercio electrónico reconocidos y confiables, ya que tienden a ser más seguros y utilizan proveedores certificados para procesar pagos. 4. Precaución con los servicios de intermediación: Sea cauteloso con los servicios de intermediación que ofrecen descuentos vinculados a la inclusión de otras personas. Esta táctica es común en el mercado electrónico y requiere un análisis cuidadoso antes de comprometerse.” [12]

Según cifras de GMS Colombia, multinacional especializada en seguridad, los sectores más vulnerables y más reciben ciberataques en América Latina son: las entidades públicas (20,0 %), seguido de la industria de alimentos (16,0 %), empresas de retail (16,0 %), el sector financiero (12,0 %) y el sector de seguros y salud (12,0 %). [13]

“La falta de autenticación robusta en las transacciones en línea puede ser un problema importante ya que permite que los ciberdelincuentes obtener información personal de los usuarios, como contraseñas, información de tarjetas de crédito/debito, para realizar transacciones fraudulentas o suplanten la identidad de los usuarios causando pérdidas financieras, poniendo en riesgo la seguridad y la privacidad de los usuarios. Cuando un usuario realiza una transacción en línea, generalmente se le pide que ingrese su información de inicio de sesión, como nombre de usuario y contraseña. Sin embargo, esta información puede ser fácilmente comprometida o robada por ciberdelincuentes a través de técnicas como

el phishing, el keylogging, la ingeniería social, ataques de hackers, denegación de servicio, ataques de malware y virus informáticos.” [14]

“Una vez que los ciberdelincuentes obtienen la información de inicio de sesión de un usuario, pueden acceder a su cuenta y realizar transacciones fraudulentas en su nombre. Esto puede resultar en la pérdida de fondos para el usuario y en la dificultad de demostrar que no ha realizado esas transacciones. Además, la suplantación de identidad es un riesgo importante relacionado con la falta de autenticación robusta en las transacciones en línea. Los ciberdelincuentes pueden utilizar la información robada de un usuario para hacerse pasar por él y realizar transacciones en su nombre. Esto no solo puede resultar en pérdidas financieras para el usuario, sino que también puede dañar su reputación y confianza en las plataformas en línea.” [15]

Por lo tanto, es crucial implementar medidas de autenticación robustas, como el uso de códigos de verificación de dos factores, el uso de biometría o la autenticación multi-factor, son formas de aumentar la seguridad en las transacciones en línea y reducir el riesgo de fraude y suplantación de identidad. Al agregar capas de seguridad adicionales, se hace más difícil para los estafadores pasar desapercibidos y realizar transacciones fraudulentas. Es importante para las empresas implementar métodos de autenticación robusta para los consumidores utilizar medidas de seguridad adicionales para proteger sus cuentas y datos personales en línea.

1.1 ARBOL DE PROBLEMAS

“Como efecto positivo a raíz de la emergencia sanitaria, se promueve utilizar las TIC (tecnologías de la información y la comunicación) para el día a día de las personas, muchas empresas tuvieron que adoptar una transformación digital de manera acelerada con el fin de mantener sus operaciones, sin embargo, no se ha tenido

suficientemente en cuenta los factores importantes relacionados con la seguridad informática. Cabe destacar que el comercio en línea en Colombia ha presentado un incremento considerable en los últimos 4 años., resaltando especialmente el año 2020 con un crecimiento de ventas en un 94.1%.” [16]

Una problemática importante de la actualidad es la manera en que se realizan las compras en línea, donde no existe un factor de autentificación o validación de titularidad suficientemente robusto que mitigue el fraude y la suplantación de identidad.

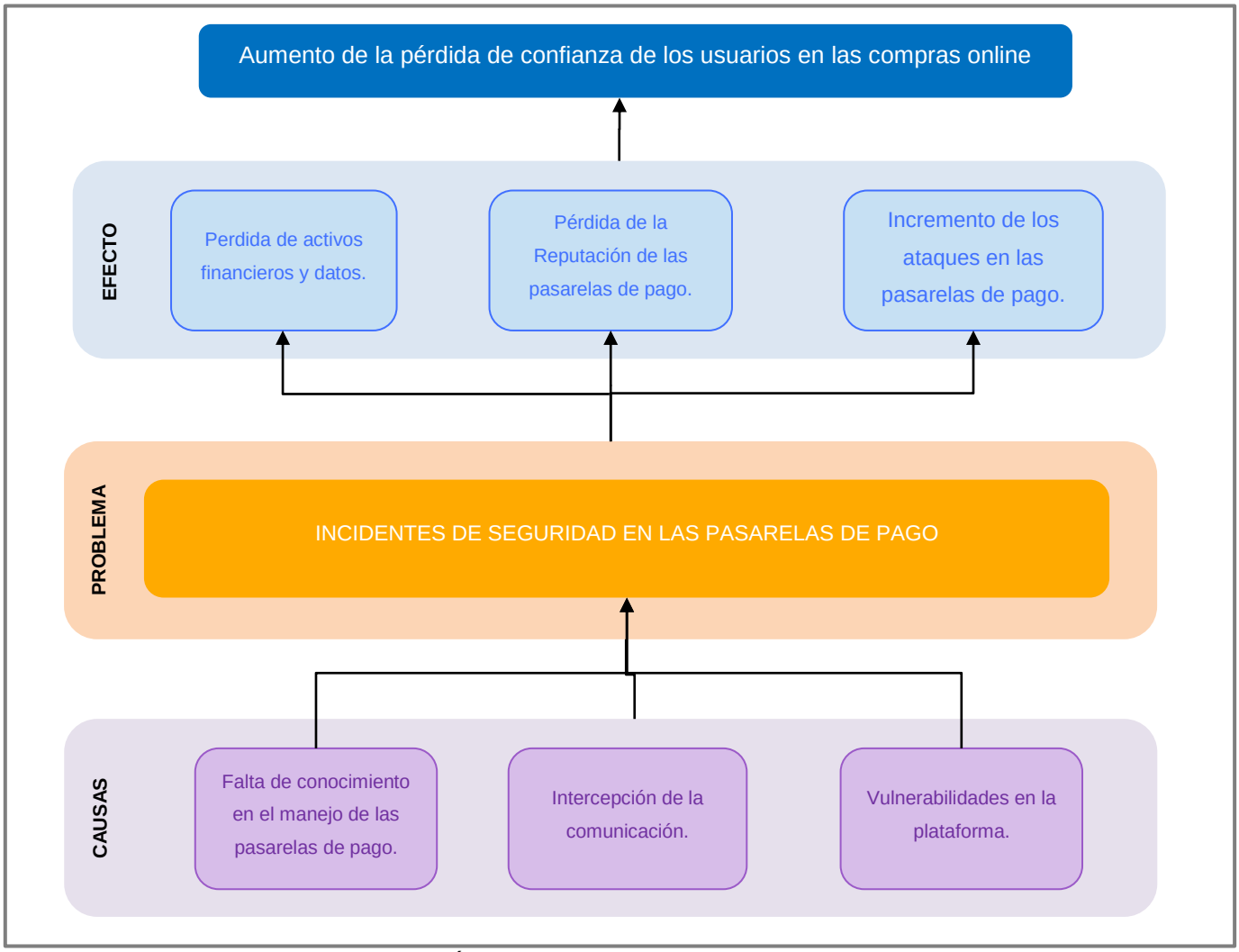

Figura 1. Árbol de Problemas. Fuente: Elaboración propia.

Objetivo General: Disminuir la pérdida de confianza de los usuarios en las compras online.

Objetivos Específicos:

- Diseñar planes de capacitación en el manejo de las pasarelas de pago.
- Mejorar la seguridad en la comunicación de las transacciones.
- Identificar y corregir vulnerabilidades en la plataforma.
- Disminución en el número de ataques a las pasarelas de pago.
- Reducción en la pérdida de activos financieros y de datos.
- Mejora en la reputación de las pasarelas de pago.
- Disminución en el número de ataques a las pasarelas de pago.

1.2 QUE SE QUIERE SOLUCIONAR

Las transacciones en línea son parte esencial en nuestra rutina. En este contexto, es esencial abordar y comprender en profundidad los incidentes de seguridad que afectan a las pasarelas de pago en línea. La seguridad en las transacciones en línea se presenta como un gran desafío en nuestro tiempo, debido a los incidentes que pueden surgir y las consecuencias que de ellos se derivan. En vista de esta realidad, la búsqueda de soluciones efectivas para mitigar estos riesgos se convierte en una prioridad ineludible en un mundo cada vez más interconectado.

Problema Central: Incidentes de seguridad en las transacciones en línea en las pasarelas de pago.

En este escenario los incidentes de seguridad en transacciones en línea, se relacionan las principales causas identificadas y las ramificaciones del problema a continuación.

Causas:

1. **Falta de conocimiento en el manejo de las pasarelas de pago,** debido a la escasa formación de usuarios y empleados para detectar y evitar situaciones de riesgos, como el phishing e ingeniería social que se hace a través de correos electrónicos fraudulentos, la manipulación psicológica de los usuarios, sitios web falsos y por hacer clic en enlaces sospechosos. Además, algunos usuarios dejan pasar por alto compartir información confidencial.

2. **Intercepción de la comunicación,** esto se debe a la falta de encriptación de la comunicación extremo a extremo, falta de una autenticación de dos factores, falta de códigos CVC dinámicos, insuficiente supervisión y monitoreo constante de las transacciones, también se identifica una respuesta ineficaz a incidentes, transacciones no autorizadas y el uso de contraseñas débiles, igualmente el acceso no controlado de socios o proveedores, los ataques externos e intrusión al sistema por parte de hackers.

3. **Vulnerabilidades en la plataforma, se identifican** métodos de autenticación y autorización débiles, también se pueden encontrar políticas de seguridad débiles/vulnerables por parte de las pasarelas de pago, mantenimiento deficiente de la infraestructura que contribuye a vulnerabilidades, el uso de dispositivos y tecnología de seguridad obsoletos, y también la falta de procesos para mitigar los incidentes.

Los incidentes de seguridad en las transacciones en línea pueden tener una amplia gama de efectos perjudiciales que van desde pérdidas de activos financieros, aumento de los índices de delitos informáticos incremento de costos operativos

administrativos, de recuperación y mitigación hasta llegar a la pérdida de confianza de los usuarios en las compras online.

Consecuencias:

1. **Perdida de activos financieros y datos,** generada por la pérdida de capital económico, el robo de información personal a los usuarios, la perdida de datos confidenciales a las entidades financieras, compras y transacciones no autorizadas. Además, ocasiona la interrupción en la operación del servicio para el usuario, produce costos de recuperación y mitigación de impacto de los incidentes, también se genera angustia emocional de usuarios por violación a su privacidad y seguridad, asimismo puede tener consecuencias legales.
2. **Pérdida de la Reputación de las pasarelas de pago,** tiene como efecto, el miedo al uso de las pasarelas de pago, produce que los usuarios cambien de entidad financiera y genera daño en la reputación de la entidad financiera.
3. **Incremento de los ataques en las pasarelas de pago,** incrementa el número de fraudes y quejas, sumada a una mala experiencia de usuario, posibles multas regulatorias por incumplimiento.

Efecto principal: Aumento de la pérdida de confianza de los usuarios en las compras online es el principal efecto negativo.

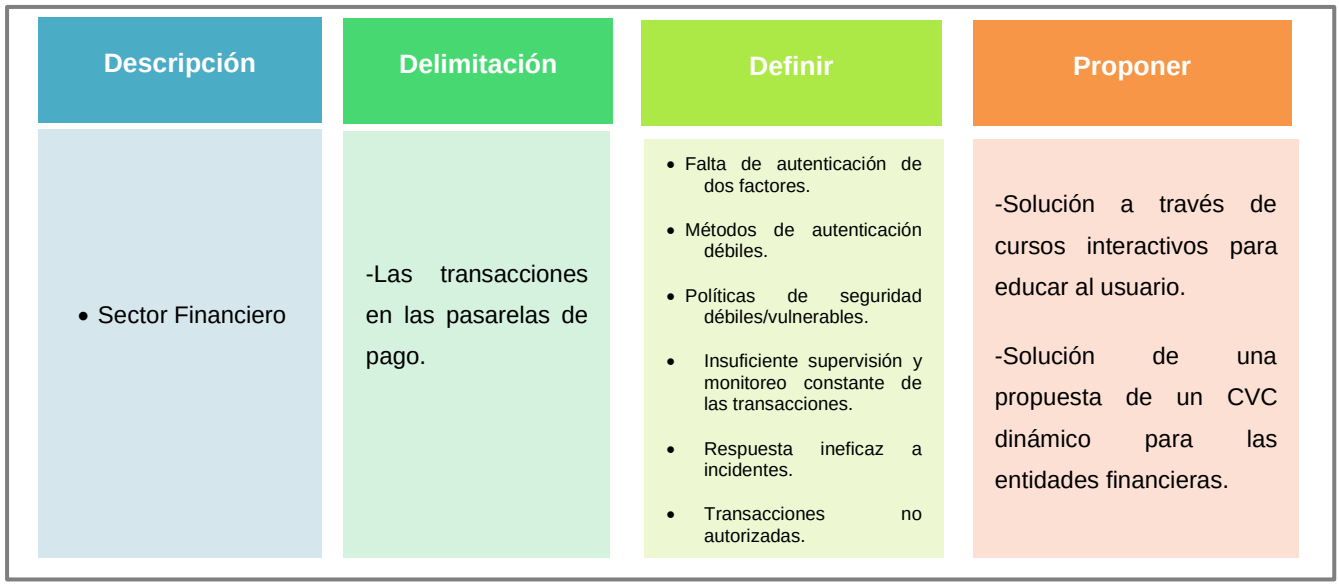

Figura 2. Delimitación del Problema. Fuente: Elaboración propia.

Descripción: "El sector de Software y Tecnologías de la Información (TI) desempeña un papel crucial en la era digital, abarcando diversas actividades que mejoran la eficiencia e innovación en diversos campos. Esto incluye desde el desarrollo de aplicaciones hasta la gestión de infraestructuras tecnológicas complejas. Con el avance tecnológico y la creciente necesidad de seguridad en el sector financiero, las empresas FinTech están constantemente mejorando sus productos en términos de calidad, seguridad y eficiencia. Utilizando blockchain, estas empresas han logrado integrar servicios financieros de manera más segura y escalable, lo que está revolucionando el sector. Blockchain permite la creación de registros digitales, mayor protección contra el fraude, eliminación de intermediarios en las transacciones y una gestión financiera más democrática a través de soluciones transaccionales, análisis de datos y automatización. Esto se traduce en servicios dinámicos y accesibles para los usuarios." [17]

“Las Fintech están transformando los servicios bancarios y financieros, generando inversión extranjera y empleo, así como modificando los servicios existentes. En América Latina, la regulación para las empresas de tecnología financiera está avanzando gradualmente en varios países, siendo México el más avanzado con regulaciones establecidas para estas compañías. Esta regulación protege a los consumidores y permite a las Fintech operar de manera libre y segura.” [18]

Delimitación: Se identifican oportunidades de mejora en el sector financiero, mediante un cambio significativo en la forma de realizar las transacciones en línea, garantizando a través de generación de códigos CVC aleatorios que puedan llegar a algún método de contacto definido por el usuario (WhatsApp, SMS, llamada, correo electrónico), el medio de recepción del código también será aleatorio.

En abril de 2021, se informó que la Dirección de Investigación Criminal e INTERPOL de Colombia identificó un alarmante aumento en los delitos informáticos, destacando la suplantación de identidad como el delito con el mayor crecimiento en el país durante el año 2020, experimentando un aumento del 409%. Mientras que en 2019 se reportaron alrededor de 300 casos de suplantación de identidad, esta cifra se disparó a 1.527 reportes en 2020. Este drástico incremento se atribuyó en gran medida a la pandemia.

“Colombia, al igual que la mayoría de los países, reconoce la importancia de proteger la titularidad de los datos personales y los derechos que les corresponden. Estos derechos están estrechamente relacionados con las actividades de tratamiento de datos, que abarcan una amplia gama de operaciones, desde la recopilación hasta la transferencia de datos personales, ya sea de forma manual o automatizada. Estas medidas buscan garantizar la seguridad y la privacidad de la información personal de los individuos.” [19]

Definir: La problemática de los incidentes de seguridad en las pasarelas de pago, afecta a las personas que gestionan sus cuentas financieras a través de aplicaciones y plataformas digitales, representan un gran desafío que amenaza tanto la seguridad de los usuarios como la integridad de las empresas en línea. Además, engloba una serie de causas en constante transformación y profundamente arraigadas que, en última instancia, minan la confianza y la eficiencia de nuestras acciones en línea.

Proponer: Se proponen una solución integral de seguridad para las transacciones en línea, enfocada a proteger tanto a los usuarios como las instituciones financieras contra amenazas cibernéticas, garantizando la confidencialidad integridad y disponibilidad de los datos financieros, a través de:

- Solución a través de cursos interactivos para educar al usuario.
- Solución de una propuesta de una CVC dinámico para las entidades financieras.

“La necesidad apremiante de salvaguardar la información y garantizar el funcionamiento óptimo en este nuevo modelo de infraestructura es innegable. La seguridad de la infraestructura en la nube se erige como un imperativo que las organizaciones deben abordar de manera efectiva para proteger su activo más valioso: los datos. Adaptar los enfoques y estrategias de seguridad tradicionales, diseñados para entornos locales, a la infraestructura en la nube se convierte en un requisito fundamental. Esto implica confiar en las herramientas, tecnologías y controles proporcionados por los proveedores de servicios en la nube para alcanzar este objetivo crucial.” [20]

Foco a la acción: Los usuarios requieren la protección de sus datos y recursos económicos para mantener la confiabilidad en las transacciones en línea.

2 IDEACIÓN DE LA SOLUCIÓN

En este mundo más digitalizado, la seguridad de la información es fundamental, la autenticación de usuarios es un pilar esencial en la protección de datos y las transacciones en línea. En este contexto, la solución de una de una CVC dinámico para las entidades financieras, se presenta como una respuesta sólida a los desafíos de seguridad cibernética en las pasarelas de pago, esta innovadora tecnología puede brindar una capa adicional de protección, fortaleciendo la seguridad de las aplicaciones y los sistemas en línea.

La educación y la concienciación de los usuarios son elementos cruciales en la lucha contra las amenazas cibernéticas. Por lo tanto, capacitar a los usuarios y empleados para para detectar situaciones de riesgos y aprender a utilizar correctamente las pasarelas de pago a través de cursos interactivos, es una estrategia efectiva para reducir de manera preventiva los riesgos asociados al utilizar las pasarelas de pago.

2.1 POR QUÉ SE PLANTEA AHORA LA SOLUCIÓN

“La prestación de servicios financieros a través de plataformas digitales está en constante aumento, particularmente en Colombia. A pesar de ello, todavía existen segmentos de la población que prefieren las interacciones en persona con las instituciones bancarias. Aun así, los bancos colombianos están adoptando gradualmente tecnologías que agilizan los procesos y mejoran la experiencia del usuario. Estas instituciones reconocen la necesidad de herramientas tecnológicas relevantes para enfrentar las demandas del mundo moderno, con un enfoque en la inteligencia artificial, el aprendizaje automático (machine learning), la tecnología blockchain y el Internet de las cosas. Estas tecnologías comparten un objetivo común: optimizar procesos, ofrecer soluciones al mercado y tener un impacto

positivo en la sociedad. La tecnología blockchain, en particular, se destaca como una innovación disruptiva con el potencial de revolucionar la gestión de datos y la seguridad de las transacciones. En un mundo digitalizado y globalizado, donde la confianza y la integridad de la información son fundamentales, la blockchain se presenta como una solución prometedora que, mediante un enfoque descentralizado y la criptografía, proporciona una manera segura y transparente de almacenar, verificar y transferir datos y activos digitales.” [21]

“En Colombia se encuentra implementada la Ley 1273 de enero de 2009, conocida como "Ley de Delitos Informáticos", proporciona un marco legal sólido para la regulación y sanción de actividades cibernéticas ilegales en el país. La pandemia ha impulsado el aumento del comercio electrónico y, por ende, de los ciberdelitos, llevando a las empresas a adoptar estrategias de transformación digital.” [22]

“El aumento en la utilización de tecnología para realizar transacciones comerciales se incorporó en la legislación nacional a través del Estatuto del Consumidor (Ley 1480 de 2011) en su séptimo título y sexto capítulo, donde se establecen mecanismos de protección y defensa para quienes utilicen el comercio electrónico de manera ocasional o regular.” [23]

“En el país se ha popularizado recientemente el término "FINTECH", que se refiere a la integración de tecnologías en el sector financiero, siguiendo la tendencia global de digitalizar una amplia gama de negocios y expandir las posibilidades y el alcance de los productos financieros. El propósito de las Fintech es eliminar barreras de entrada, reducir costos y acortar los tiempos de espera para adquirir productos financieros, todo esto a través del uso de diversas herramientas tecnológicas de información y comunicación.” [24]

“Las pasarelas de pago son sistemas que permiten a los usuarios llevar a cabo transacciones financieras en línea. Surgieron en la década de 1990, coincidiendo con el auge de las tiendas en línea y el crecimiento de las transacciones comerciales en Internet. En sus inicios, se presentaron pasarelas como CyberCash y Digicash, que facilitaron los pagos en línea con tarjetas de crédito. A principios de los años 2000, empresas como PayPal y Amazon Payments introdujeron alternativas de pago en línea, como la transferencia electrónica y el uso de cuentas bancarias. Luego, surgieron las pasarelas de pago móviles, como Square y Google Wallet, que permitieron a los consumidores realizar pagos a través de dispositivos móviles. La implementación de pasarelas de pago en línea es considerada una excelente solución para las empresas debido a su versatilidad y seguridad en los métodos de pago. Estos sistemas son escalables y se adaptan a diversos canales de venta sin importar la tecnología o la demanda de productos. La seguridad desempeña un papel fundamental en las pasarelas de pago, ya que deben contar con sistemas de cifrado, PCI-DSS y Webhook para garantizar la seguridad de los datos del cliente. La integración con webhooks permite la comunicación automatizada entre aplicaciones y es esencial para la confirmación de pagos y la gestión de pedidos. Las pasarelas de pago se han implementado en diversos sectores, como la educación virtual, donde han simplificado los procesos de pago y facturación, además de proporcionar información estadística sobre la rentabilidad de los cursos. Antes de implementarlas, se recomienda investigar las experiencias exitosas en otros países para comprender posibles problemas y soluciones.” [25]

La figura 3 presenta un análisis del crecimiento de las pasarelas de pago en el país (Colombia) desde el 2018 hasta el 2019, destacando el comportamiento de las pasarelas de pago más relevantes y la clasificación de usuarios basados en el número de transacciones anuales entre otros aspectos.

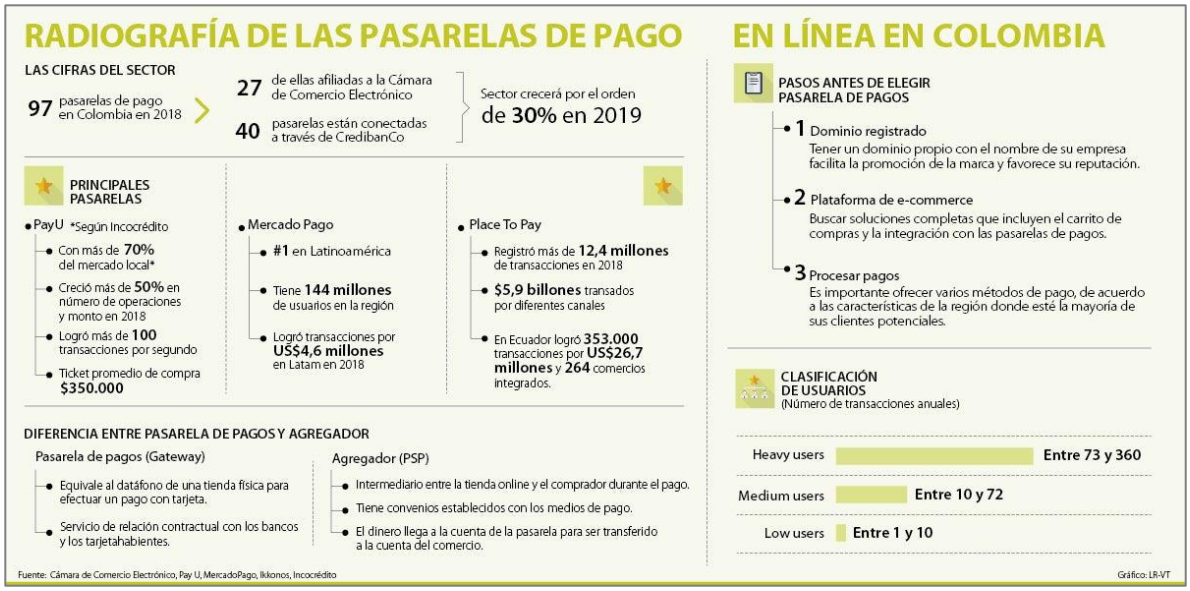

Figura 3. Radiografía de las pasarelas de pago en línea en Colombia Fuente: Tomado de larepublica.co.

“En Colombia, existen alrededor de 97 pasarelas de pago, según la Cámara Colombiana de Comercio Electrónico (CCE). Estas pasarelas se dividen en dos tipos: las pasarelas de pago (gateways) y los agregadores (PSP), que actúan como intermediarios entre las tiendas en línea y los compradores durante el proceso de pago. PayU lidera el mercado de pasarelas de pago a nivel local, con más del 70% de la cuota de mercado.” [26]

“La pandemia de COVID-19 impulsó el desarrollo de la metodología Frictionless en el comercio, que permite la autenticación sin la necesidad de una constante interacción con el comprador. Esto ha resultado en una mayor adopción de experiencias de compra fluidas, que requieren la introducción de nuevos métodos de pago, la colaboración con socios tecnológicos, la gestión de políticas de

seguridad y la salvaguardia de los datos capturados, registrados y necesarios durante las transacciones. La exposición al fraude digital es un problema en aumento, y las empresas, sin importar su tamaño, deben tomar medidas para mitigar los riesgos. En momentos de alta demanda, como el Cyberlunes o el Black Friday, la solidez de las plataformas de comercio en línea es fundamental, al igual que la promoción de una cultura de seguridad en la organización. Las empresas deben implementar políticas de seguridad y protección de datos, además de educar a los clientes sobre los diversos tipos de fraude y cómo protegerse. Todo esto debe llevarse a cabo en cumplimiento de las regulaciones locales y globales de seguridad y privacidad de datos, como el GDPR y Hábeas Data.” [27]

" En América Latina, los Servicios Financieros Digitales han experimentado avances notables, según lo señala Anif. Entre los progresos en la oferta digital se encuentran las transferencias bancarias, los pagos de servicios públicos y los giros. No obstante, solo el 53% de los bancos permite abrir cuentas de ahorro en línea, en contraste con el 80% en España. Además, únicamente el 39% proporciona opciones digitales para otros tipos de depósitos, como los Certificados de Depósito a Término (CDT) o los Certificados de Depósito de Ahorro a Término (CDAT). El informe también resalta que los usuarios de servicios financieros digitales están mayormente concentrados en la población relativamente joven, principalmente entre las edades de 25 y 45 años. Esto sugiere la posibilidad de un mayor crecimiento en la adopción y profundización de servicios digitales a medida que esta población aumenta en número y riqueza. Otro aspecto relevante que destaca el informe es que el 48% de los bancos en América Latina destinan entre un 10% y 20% de su presupuesto a inversiones en tecnología e innovación, y un 17% invierte más del 20%, mientras que solo un 5% asigna menos del 5% de su presupuesto a la innovación.” [28]

“Actualmente el mercado de la industria de pagos electrónicos demanda una disponibilidad del servicio 24 horas al día, los 7 días de la semana, durante todo el año. Esto significa que no pueden permitirse que el servicio presente interrupciones, ya sean pequeñas o, en el peor de los casos, deben ser solucionadas de manera extremadamente rápida. En la actualidad, cualquier interrupción del servicio puede tener implicaciones económicas, como incumplimientos de acuerdos de servicio, y aún más críticamente, puede afectar la reputación de una entidad.” [29]

“La seguridad en la banca digital es un tema de gran relevancia debido a los efectos negativos que se están experimentando en la actualidad, incluyendo robo de información, delitos financieros para préstamos o compras en línea, entre otros.

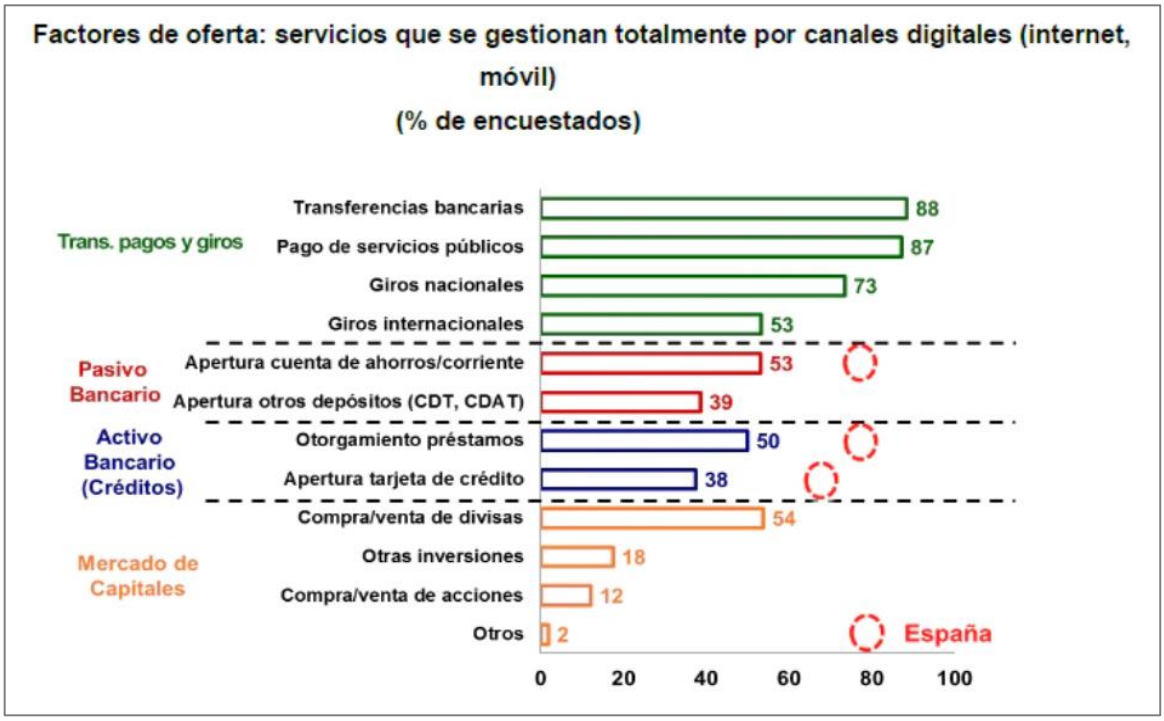

Figura 4. Servicios gestionados por canales digitales Fuente: Anif y Feleban

Esto genera preocupaciones e incertidumbre entre los clientes en lo que respecta al uso de aplicaciones en línea. Por lo anterior, la seguridad en los sistemas de

información financiera o de los datos personales, son los aspectos técnicos que avalan la integridad, la confidencialidad, la certificación y aprobación de las transacciones que permiten el cumplimento de los requisitos legales y las prácticas útiles en el tema de la confidencialidad, con esto se busca principalmente la confianza y fidelidad del cliente. Todo esto conlleva, a favorecer la comodidad a los clientes al permitirles realizar operaciones desde cualquier lugar y evitar la necesidad de visitar oficinas físicas, busca ganar la confianza de los usuarios al implementar medidas de seguridad que verifiquen la identidad del cliente registrado. La inseguridad en la banca digital afecta la imagen que el banco proyecta ante sus clientes y resalta la importancia de garantizar la seguridad en este entorno.” [30]

“Nunca se debe divulgar el código CVV por correo electrónico, ya que esto podría facilitar a los delincuentes cibernéticos realizar un uso indebido de la tarjeta si tienen acceso al número de tarjeta, PIN y fecha de vencimiento. El CVV desempeña un papel crucial en la seguridad de las compras en línea, ya que su ingreso es necesario para completar la transacción. Este código agrega una capa adicional de confirmación de la identidad del titular de la tarjeta y no se genera de forma automática. Al efectuar compras en línea, es esencial seguir medidas de prevención de fraudes, como utilizar plataformas de pago seguras y sitios web con el código de seguridad HTTPS y el símbolo de un candado que garantiza la protección de la transacción.” [31]

“El CVV, también conocido como código valor de verificación o validación (Card Verification Value), es un conjunto de tres o cuatro dígitos que se encuentra en la parte posterior de la tarjeta. El nombre de este código puede variar según la empresa de tarjetas de crédito y también puede ser denominado código de verificación de la tarjeta o CVC (Card Verification Code), código de seguridad de la tarjeta o código personal de seguridad. Además de los dígitos principales que identifican el número de la tarjeta, existen otros dos grupos de números con funciones estrictas de seguridad. Estos dos códigos son la fecha de caducidad, que

se expresa en formato MM/AA (mes/año) y señala la fecha límite de uso de la tarjeta, y el CVV o CVC. Ambos tienen la finalidad de demostrar que la persona que realiza la compra posee la tarjeta físicamente y no solo el número, lo que previene posibles transacciones fraudulentas.” [32]

“Existen diferentes tipos de CVV o CVC en una tarjeta, aunque su denominación puede variar, su función principal sigue siendo la seguridad del usuario al realizar compras en línea. El CVC tipo 1 de una tarjeta se encuentra en la banda magnética y es leído automáticamente por terminales de punto de venta (TPV) o lectores de tarjetas al insertarla o realizar el contacto. Por otro lado, el CVV tipo 2 de una tarjeta, compuesto por tres dígitos y ubicado en la parte posterior de la tarjeta, desempeña un papel fundamental en las compras en línea y tiene como objetivo prevenir el uso indebido de la tarjeta.” [33]

“Para realizar compras en línea, es esencial ingresar el código de verificación de la tarjeta, conocido como CVV o CVC. Tradicionalmente, este número de tres dígitos se encontraba impreso de manera estática en el reverso de la tarjeta. Sin embargo, los avances tecnológicos han dado paso a una solución más segura, el CVV dinámico. Con esta tecnología, cada vez que el usuario efectúe una compra en línea, la entidad financiera generará un código numérico de tres cifras de forma aleatoria con una vigencia de aproximadamente entre cinco y diez minutos. Esta medida aumenta la seguridad al realizar compras en tiendas en línea, ya que evita el posible uso fraudulento de la tarjeta, protegiendo así los datos del usuario.” [34]

2.2 SECTOR OBJETIVO

El ámbito de estudio de esta investigación se enfoca en el sector financiero, específicamente en las pasarelas de pago en línea. Este sector se ve directamente impactado por aspectos relacionadas a la seguridad de las transacciones en línea. Comprender y analizar los incidentes de seguridad en las transacciones en línea, con el fin de abordar desafíos multidimensionales que amenazan tanto la seguridad de los usuarios como la integridad de las empresas que operan en línea.

2.2.1 Definición Del Sector

Las pasarelas de pago en línea son esenciales en el ámbito del comercio electrónico. Estas pasarelas permiten a individuos y empresas realizar transacciones financieras en línea de manera segura y eficiente. Sin embargo, las Fintech desempeñan un papel clave en el comercio electrónico al proporcionar soluciones financieras y tecnológicas que mejoran la eficiencia, la seguridad y la experiencia del usuario en las transacciones online. Su relación con las pasarelas de pago permite a las empresas de comercio electrónico ofrecer una variedad de opciones de pago mejorando la gestión de las transacciones en línea.

El crecimiento de estas pasarelas se ha visto impulsado por la creciente demanda de comercio electrónico, aunque también han surgido desafíos de seguridad, como el fraude cibernético y la suplantación de identidad. Para abordar estos desafíos, dentro del sector se han desarrollado diversas medidas de seguridad, como la encriptación SSL/TLS, la tokenización y la verificación en dos pasos, entre otras. Estas medidas buscan proteger la información financiera y personal de los usuarios y garantizar la integridad de las transacciones en línea. Estos segmentos son parte integral del sector de servicios de TI ejerciendo

un papel clave al abracar una amplia gama de servicios destinados a atender las necesidades de las entidades financieras.

2.2.2 Descripción Del Sector

El sector del comercio electrónico específicamente las pasarelas de pago en línea, se caracteriza por ser un componente fundamental del entorno financiero digital. Estas plataformas permiten a individuos y empresas realizar compras, pagos de facturas, transferencias y transacciones financieras de manera rápida, segura y eficiente a través de la web. Estas pasarelas, a menudo son ofrecidas por empresas FinTech, las cuales han experimentado un crecimiento significativo en respuesta a la creciente demanda de comercio electrónico, sin embargo, este crecimiento también ha expuesto al sector a una creciente amenaza de incidentes de seguridad, que afectan tanto a los usuarios como a las empresas. La seguridad es esencial para mantener la confianza de los usuarios y garantizar un entorno de comercio electrónico seguro y próspero en el mundo digital actual, fortalecer la seguridad en este sector, implica la implementación de políticas de seguridad más robustas, la adopción de tecnologías avanzadas para prevenir el fraude, robo de información, robo de activos económicos, garantizar la integridad de los datos financieros y la educación de los usuarios.

Los incidentes de seguridad en las pasarelas de pago se presentan como un problema complejo y en constante evolución, que involucra causas arraigadas y diversas consecuencias perjudiciales. En este sector, es fundamental asegurar la confidencialidad, integridad y accesibilidad de la información financiera, así como mantener la seguridad en las operaciones en línea.

Este sector se caracteriza por su diversidad y se divide en varios segmentos clave:

- Tipo de Servicio: Incluye servicios profesionales, como la integración de sistemas y consultoría, así como servicios gestionados que ofrecen soluciones de TI continuas y supervisión.
- Tamaño de la Empresa: Se adapta tanto a grandes empresas como a pequeñas y medianas empresas (PYMEs), brindando soluciones y servicios que se ajustan a las dimensiones y necesidades de cada una.
- Industria del Usuario Final: Se dirige a una variedad de industrias, como telecomunicaciones, servicios financieros (BFSI), atención médica, venta minorista, manufactura y el sector gubernamental, adaptando soluciones específicas a los desafíos y requisitos de cada sector.
- Geografía: Aborda mercados en todo el mundo, lo que refleja su alcance global.

La evaluación y proyección del mercado en esta industria se fundamenta en el crecimiento económico para cada uno de los segmentos mencionados, lo que destaca la magnitud y la importancia de este sector en la economía global. [35]

2.2.3 Aplicaciones Del Sector

Las aplicaciones de las pasarelas de pago en línea son variadas y cubren una amplia gama de transacciones financieras. Esto incluye la adquisición de productos y servicios en línea, el pago de facturas, la transferencia de fondos entre cuentas, la contribución a organizaciones benéficas y el procesamiento de pagos para empresas de comercio electrónico. Además, estas pasarelas permiten a las empresas recibir pagos de manera eficaz, ya sea a través de tarjetas de crédito, débito, transferencias bancarias u otros métodos de pago en línea.

Algunas de las aplicaciones de las pasarelas de pago que se pueden encontrar dentro de la amplia variedad de

- **Comercio electrónico:** Las pasarelas de pago ofrecen soluciones de procesamiento de pagos en línea que permiten a las entidades de comercio electrónico aceptar pagos en línea de sus clientes, Facilitan transacciones con tarjetas de débito, crédito, y otros métodos de pago en línea, lo que es fundamental para el éxito del comercio electrónico.
- **Banca en línea:** Las instituciones financieras utilizan pasarelas de pago para permitir que sus clientes realicen transferencias de fondos, pagos de facturas y transacciones entre cuentas de manera segura a través de plataformas de banca en línea.
- **Billeteras digitales:** El desarrollo de billeteras digitales permite ofrecer soluciones de pago móvil, facilitando a los usuarios realizar transacciones y compras desde sus dispositivos móviles a través de aplicaciones de billetera digital, códigos QR y tecnología NFC (Near Field Communication).
- **Financiamiento en línea:** Algunas instituciones financieras ofrecen sus servicios permitiendo solicitar créditos, tarjetas de crédito, abrir CDT, también; permiten a las empresas de comercio electrónico acceder a capital para expandir sus operaciones, comprar inventario o invertir en marketing. Esto puede ser fundamental para el crecimiento de las empresas de comercio electrónico.
- **Seguridad y prevención de fraudes:** Las fintech también desempeñan un papel importante en la seguridad de las transacciones en línea, proporcionando soluciones de detección de fraudes y autenticación biométrica para proteger a las empresas y a los consumidores de posibles amenazas cibernéticas.

- **Análisis de datos y gestión financiera:** Algunas fintech ofrecen herramientas de análisis de datos y gestión financiera que ayudan a las empresas de comercio electrónico a comprender mejor su flujo de efectivo, administrar sus finanzas y tomar decisiones basadas en datos para optimizar sus operaciones.
- **Pagos recurrentes:** Las pasarelas de pago facilitan la programación de pagos recurrentes, lo que es útil en casos como el pago de suscripciones mensuales, préstamos y facturas periódicas.
- **Transferencias internacionales:** Las pasarelas de pago permiten la transferencia de fondos entre diferentes países, lo que es fundamental para el comercio internacional y las remesas.
- **Pagos a proveedores y nóminas:** Las empresas utilizan pasarelas de pago para realizar pagos a proveedores y empleados de manera eficiente y segura, lo que reduce la necesidad de cheques y transferencias bancarias tradicionales.
- **Plataformas de criptomonedas:** En el ámbito de las criptomonedas, las pasarelas de pago permiten a los usuarios comprar, vender e intercambiar criptomonedas de forma segura.

En resumen, las pasarelas de pago son una parte fundamental de la infraestructura financiera y desempeñan un papel importante al facilitar la ejecución de transacciones electrónicas, tanto en el comercio electrónico como en una variedad de otros contextos financieros. Ayudan a garantizar la seguridad y la eficiencia en la transferencia de fondos y en la realización de transacciones en línea y fuera de línea.

En lo que respecta a la seguridad en las transacciones en línea, se pueden encontrar diversas aplicaciones y prácticas relacionadas con la seguridad de pasarelas en línea. Estas acciones son cruciales para asegurar la salvaguardia de

los datos financieros y personales de los usuarios. Algunas de las tecnologías y prácticas habituales son:

- **Encriptación SSL/TLS:** Se emplea la capa de sockets seguros (SSL) o su evolución, el Transport Layer Security (TLS), para cifrar la interacción entre el navegador del usuario y el servidor de la entidad que ofrece la pasarela de pago, garantizando que la información transmitida esté resguardada contra el acceso no autorizado.

- **Tokenización:** En lugar de almacenar datos de tarjetas de crédito en un sistema, se utilizan tokens únicos que representan esa información, con el objetivo de reducir riesgos asociados al almacenamiento de datos sensibles.

- **Verificación en dos pasos (2FA):** Se implementa para proporcionar una capa adicional en la seguridad, requiriendo que los usuarios proporcionen información adicional, como un código enviado al teléfono móvil, adicional a su contraseña, para verificar su identidad.

- **Prevención de fraudes y análisis de comportamiento:** Herramientas y algoritmos avanzados para analizar patrones de comportamiento y detectar actividades inusuales o sospechosas que puedan indicar intentos de fraude.

- **Cumplimiento con PCI DSS**: Este Estándar de Seguridad de Datos del Sector de Tarjetas de Pago (PCI DSS) establece requisitos para garantizar la seguridad de la información de tarjetas de crédito. Las pasarelas de pago deben cumplir con estos estándares para procesar pagos de manera segura.

- **Firewalls y Seguridad de Red:** implementación de firewalls y otras estrategias de seguridad de la red con el fin de salvaguardar contra amenazas provenientes del exterior.

- **Actualizaciones regulares y parches de seguridad:** Actualizar constantemente todos los sistemas y programas con las más recientes correcciones de seguridad, como medida de resguardo ante vulnerabilidades ampliamente reconocidas.

- **Auditorías de seguridad:** Las auditorías en la seguridad de forma regular permite identificar y corregir posibles vulnerabilidades en el sistema.

- **Geofencing y restricciones de IP:** Limitar el acceso a la pasarela de pago desde ubicaciones geográficas específicas o direcciones IP autorizadas para prevenir accesos no autorizados.

- **Gestión de claves criptográficas:** Asegurarse de que las claves utilizadas para la encriptación se gestionen de manera segura y se actualicen regularmente.

“Es importante tener en cuenta que la seguridad de las transacciones en línea es un esfuerzo continuo, y las empresas deben adaptarse constantemente a nuevas amenazas y vulnerabilidades mediante la a través de buenas prácticas de seguridad disponibles.” [36]

2.2.4 Relación De Las Aplicaciones Con La Propuesta

El sector financiero y la tecnología de la información están intrínsecamente relacionados, ya que forman la base esencial para el desarrollo, funcionamiento y prestación de servicios de las pasarelas de pago. Asegurar la protección de los datos y los activos económicos de los usuarios en transacciones en línea es de suma importancia, ya que esto contribuye a incrementar la confianza de los usuarios al utilizar estas pasarelas. La implementación de políticas de seguridad sólidas, orientadas a preservar la integridad, confidencialidad y disponibilidad de los datos, se ha convertido en una prioridad ineludible para las entidades financieras.

Abordar los incidentes de seguridad en las transacciones en línea a través de las pasarelas de pago es de vital relevancia, dado que cualquier vulnerabilidad en la seguridad podría tener consecuencias graves, como la pérdida de activos financieros, la divulgación de información confidencial, el robo de identidad y la interrupción de los servicios en línea. La relación entre las aplicaciones del sector y esta propuesta es directa, ya que la solución busca fortalecer la seguridad de dichas aplicaciones y mitigar los riesgos asociados con las transacciones en línea. Esto implica la aplicación de medidas de seguridad, como la autenticación de dos factores, la generación de códigos CVC dinámicos y la educación de los usuarios acerca del uso de las pasarelas de pago, con el objetivo de proteger tanto a los usuarios como a las empresas que operan en el sector. Al reforzar la seguridad de estas aplicaciones, se busca preservar la confianza de los usuarios y asegurar que el sector del comercio electrónico continúe prosperando en un entorno digital cada vez más complejo.

2.3 TENDENCIAS DEL SECTOR

“En los últimos años, el sector de las pasarelas de pago en línea ha experimentado un continuo y dinámico crecimiento, impulsado en gran medida por el auge del comercio electrónico y los avances tecnológicos. Con el aumento constante de usuarios que realizan transacciones en línea, las empresas de este sector han trabajado en fortalecer sus servicios para atraer y retener a estos usuarios, ofreciéndoles más opciones para gestionar sus finanzas de manera digital.

En Colombia, los pagos en línea se concentran principalmente en categorías como tecnología y productos electrónicos, ropa y calzado, artículos deportivos y minoristas, con un gran potencial de crecimiento. Se proyecta un aumento del 71% para el año 2025, con aproximadamente 34 millones de usuarios en la actualidad. Estas tendencias reflejan el significativo crecimiento del sector y su influencia en la forma en que se llevan a cabo las transacciones en línea. Esto se puede observar en la figura 5, que muestra las tendencias de los métodos de pago más utilizados en el comercio electrónico en Colombia durante el año 2023.” [37]

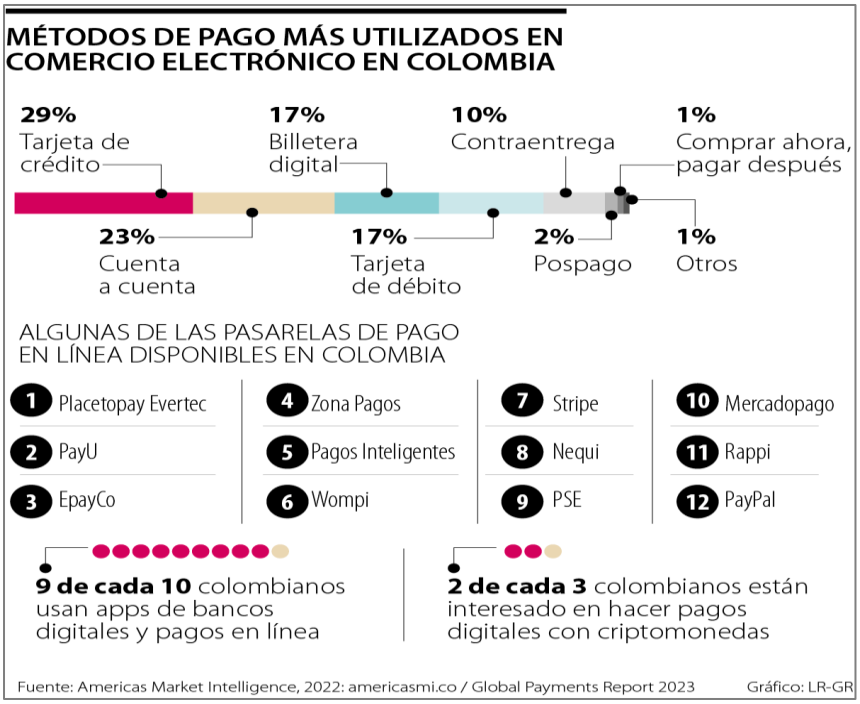

Figura 5 Métodos de pagos más utilizados en comercio electrónico en Colombia Fuente: America MArket intelillence 2022

“En cuanto a las tendencias en el sector de las pasarelas de pago, se observa que la Generación Z está desempeñando un papel cada vez más relevante en el ámbito de las transacciones en línea al impulsar el uso de pasarelas de pago. Los pagos corporativos B2B están experimentando cambios positivos gracias a la influencia de la tecnología y las Fintech, que ofrecen opciones de pago más simples, rápidas y económicas, centrándose en la tecnología digital. Las tecnologías web3, como blockchain, criptomonedas, NFT y el Metaverso, están introduciendo innovaciones significativas que están transformando la manera en que los bancos deben proporcionar productos y servicios de moneda digital. La popularización de las billeteras móviles ha impulsado el aumento de los pagos móviles y la gestión de entradas para eventos, llaves de autos, reservas de hoteles, programas de fidelidad, identificación digital, métodos de pago en el transporte público, registros de vacunación y mucho más. Estas nuevas soluciones de tarjetas digitales ofrecen oportunidades para que los proveedores de pagos revisen e inviertan en estrategias de billetera y otras capacidades digitales para promover su activación y uso. Además, la consolidación del open banking, respaldada por tecnologías habilitadoras, fomenta la estandarización de interfaces y protocolos con el objetivo de garantizar la seguridad y la interoperabilidad entre los diversos actores del sistema financiero. También busca impulsar la competencia y mejorar la calidad de los servicios financieros disponibles tanto para consumidores como para empresas”. [38]

“El sector de las pasarelas de pago en línea se encuentra en constante evolución para satisfacer las demandas cambiantes de seguridad, comodidad y eficiencia. Estas tendencias están moldeando la forma en que realizamos transacciones en línea y tienen un impacto significativo en la confianza del usuario y el crecimiento continuo del comercio electrónico en un mundo digital cada vez más complejo. Esta preocupación es un factor fundamental para el desarrollo y progreso del sector, esta tendencia de integración es relevante en un período de crecimiento de las transacciones electrónicas.” [39].

La innovación tecnológica a través de inteligencia artificial, el aprendizaje automático y la cadena de bloques, han transformado la forma en que realizamos transacciones en línea, estas tecnologías han mejorado la seguridad de las transacciones, creando una experiencia de usuario más personalizada y sin complicaciones. Este cambio ha sido fundamental para fortalecer la confianza del usuario en las transacciones en línea y para impulsar el crecimiento continuo del comercio electrónico en un mundo digital en constante expansión.

La integración de estas tendencias en las pasarelas de pago es esencial en un momento en el que las transacciones electrónicas están experimentando un crecimiento significativo. La preocupación por la seguridad de las transacciones es un factor fundamental para el desarrollo y progreso del sector, donde la adaptación de tecnologías emergentes y la creación de soluciones de pago más seguras y convenientes están en el centro de esta evolución. La capacidad de satisfacer estas demandas cambiantes no solo impacta la experiencia del usuario, sino que también moldea el panorama del comercio electrónico, marcando pautas sobre cómo se llevan a cabo las transacciones en un entorno digital complejo y en constante cambio.

La confianza del usuario es crucial en este entorno digital en rápida evolución, la capacidad de las pasarelas de pago para ofrecer seguridad y eficiencia en las transacciones en línea influye directamente en la confianza del consumidor. Además, la integración de tecnologías innovadoras no solo proporciona un marco más seguro, sino que también contribuye al desarrollo de un ecosistema de pagos más eficiente y adaptable. Esta evolución es esencial para mantener la relevancia en un período de crecimiento exponencial de las transacciones electrónicas, donde la confianza y la seguridad se han convertido en pilares fundamentales para el éxito continuo del comercio en línea.

La evolución constante de las pasarelas de pago en línea refleja una búsqueda incesante de soluciones que se alineen con las expectativas y necesidades de los consumidores en un mundo digital en constante cambio. La integración de tecnologías emergentes no solo está transformando la forma en que se llevan a cabo las transacciones, sino que también está redefiniendo la confianza del usuario y el crecimiento del comercio electrónico. Este enfoque en la seguridad, la comodidad y la eficiencia es fundamental para mantener la relevancia y la competitividad en un entorno donde la tecnología sigue siendo un motor clave del progreso económico.

2.4 ANALISIS DE MERCADO

“El mercado de pasarelas de pago es un sector en expansión que se ve impulsado por el crecimiento del comercio electrónico y la adopción de sistemas de pago móvil. Estas pasarelas permiten a las empresas aceptar pagos a través de tarjetas de crédito, débito y otros métodos de pago. El mercado global de pasarelas de pago experimentó un valor de 13.97 mil millones de dólares para el 2023 proyectando un alcance los 29.89 mil millones de dólares para 2028, con una tasa de crecimiento anual compuesta del 16.43% para el pronóstico de este período de (2023 hasta 2028). Este aumento en el mercado de pasarelas de pago se atribuye a varios factores, entre los que se incluyen el crecimiento acelerado del comercio electrónico a nivel mundial, lo que genera una mayor demanda de estos servicios. La adopción de pagos móviles también está ganando popularidad, lo que crea nuevas oportunidades para las pasarelas de pago. Además, la creciente globalización de las empresas, que expanden sus operaciones a nivel internacional, exige la disponibilidad de pasarelas de pago capaces de aceptar transacciones en diversas monedas y países.” [40]

Las pasarelas de pago para comercio electrónico B2B en Colombia, son herramientas que facilitan a los negocios electrónicos recibir pagos de tarjetas de

débito, crédito, y otros medios de pago, son importantes para los negocios electrónicos porque facilitan que los clientes realicen pagos de forma segura y conveniente. Hay muchas pasarelas de pago disponibles en Colombia, cada una con sus propias características y tarifas algunas pasarelas de pago para comercio electrónico B2B en Colombia son: PayU, PSE, PayPal, AmazonPay, Stripe, Payline Data, Authorice.Net, 2checkout, Braintree, BlueSnap, PayPro Global y Swipe. [41]

“Uno de los aspectos más preocupantes destacados en diferentes artículos es la disparidad demográfica en las tasas de fraude de identidad. Según el informe de la FTC, las personas de 65 años tienen más probabilidades que las personas de 18 a 29 años de sufrir fraude de identidad. Este hallazgo desafía la percepción convencional de que los jóvenes son más propensos a ser víctimas de este tipo de delitos, subrayando la necesidad de estrategias específicas de protección para la población de edad avanzada.” [42]

“Además, la relación entre el nivel de ingresos y la vulnerabilidad al fraude de identidad también emerge como un tema significativo. El informe de la oficina del fiscal general de los Estados Unidos revela que las personas con ingresos anuales de menos de $75,000 tienen más probabilidades que las personas con ingresos anuales de más de $100,000 de sufrir fraude de identidad. Este dato refleja la realidad de que la seguridad financiera no es una garantía contra los ciberataques, y destaca la importancia de la educación financiera y la conciencia en todos los estratos sociales.” [43]

“En los diversos estudios analizados, se observa que aquellos individuos que mantienen una presencia activa en las redes sociales están más susceptibles a convertirse en víctimas de delitos cibernéticos. Este hallazgo resalta la imperante necesidad de enfocarse en la protección de datos y en garantizar la seguridad de las transacciones realizadas a través de plataformas digitales.” [44]

2.5 ÁRBOL DE OBJETIVOS

El siguiente árbol de objetivos se plantea con el propósito de enfrentar y solucionar los desafíos vinculados a la seguridad en las transacciones en línea, con la meta final de mantener la confianza de los usuarios y reforzar la seguridad en el ámbito digital. Este es un recurso valioso que facilita la comprensión y la planificación de acciones para prevenir, detectar y responder a incidentes de seguridad en las pasarelas de pago.

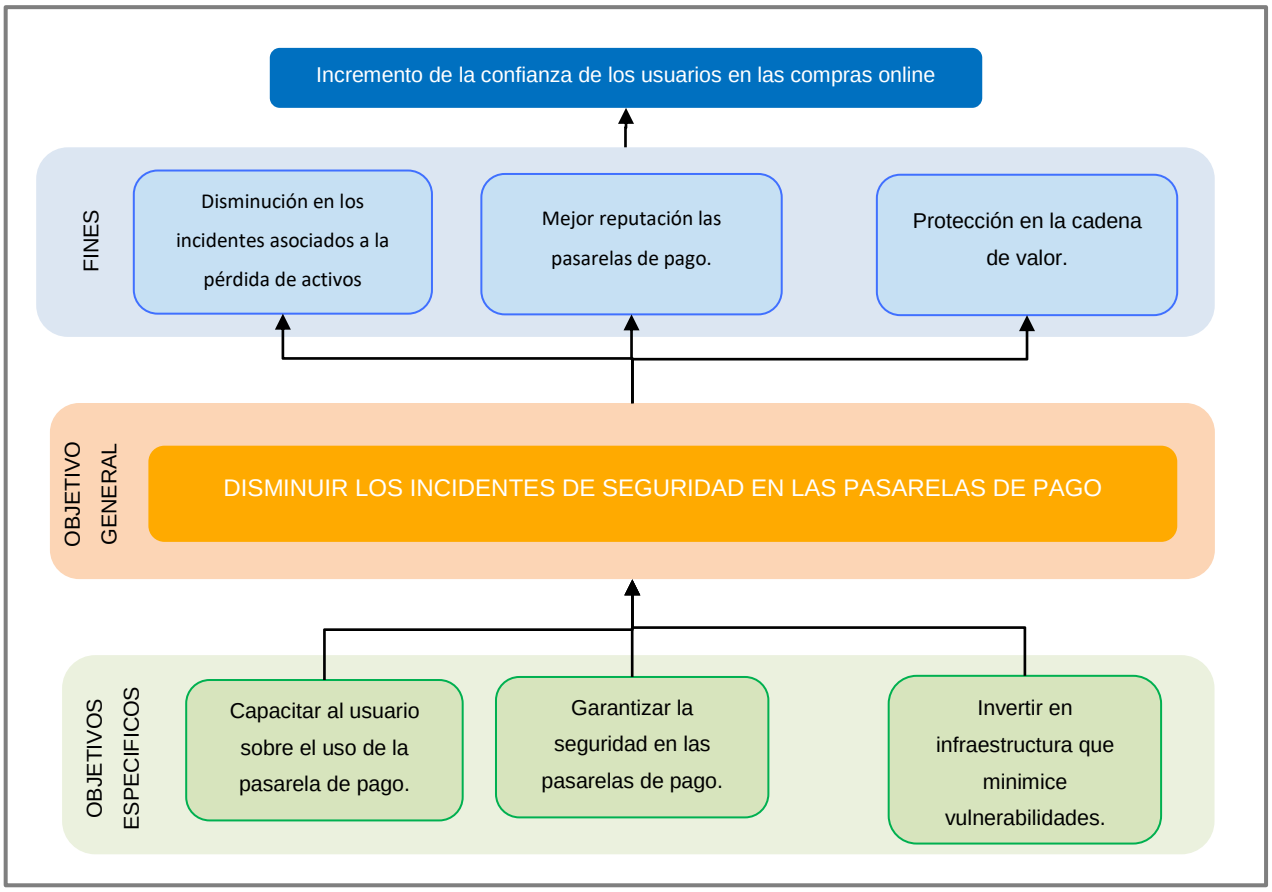

Figura 6. Árbol de objetivos. Fuente: Elaboración propia.

En el árbol de objetivos se han planteados los siguientes **objetivos específicos**:

- **Capacitar al usuario sobre el uso de la pasarela de pago,** desarrollando recursos educativos interactivos y de fácil acceso que guíen a los usuarios en el uso efectivo de la pasarela de pago, incluyendo tutoriales de paso a paso y videos explicativos. También, sesiones de capacitación en línea, campañas de sensibilización sobre seguridad, entrenamiento regular en prácticas seguras de pago y comunicación proactiva sobre posibles riesgos y medidas de protección que promuevan la conciencia y la responsabilidad en todos los niveles de la entidad financiera y entre los usuarios finales.

- **Garantizar la seguridad en las pasarelas de pago,** usar tecnologías de vanguardia que permitan mitigar los incidentes que se llegan a presentar en pasarelas de pago, implementando una capa de seguridad adicional que permita validar la identidad del usuario.

- **Invertir en infraestructura que minimice vulnerabilidades,** invertir en la actualización y mejora de la infraestructura tecnológica para reducir las vulnerabilidades potenciales, la adopción servicios informáticos en la nube, la implementación de medidas proactivas para mitigar posibles amenazas de seguridad, realizar auditorías regulares y evaluaciones de seguridad para identificar posibles brechas o puntos débiles en las pasarelas de pago, realizar mejoras continuas y ajustes en tiempo real para mantener la integridad y la protección de los sistemas de pago.

Al expandir estos objetivos específicos, se puede fortalecer el enfoque en la capacitación, la seguridad y la infraestructura para construir un entorno de pasarelas de pago más sólido y confiable.

Con el fin de lograr el objetivo general: Disminuir Los Incidentes De Seguridad En Las Pasarelas De Pago en un 80%.

Para lograr los fines:

- **Disminución en los incidentes asociados a la pérdida de activos,** capacitar a los usuarios sobre el uso adecuado de las pasarelas de pago e implementar medidas sólidas de seguridad permite reducir la probabilidad de incidentes de seguridad como el robo de activos económicos, robo de datos financieros, minimizar el riego de fraude, lo que lleva a la disminución en la pérdida de activos tanto para los usuarios como las entidades financieras.

- **Mejor reputación las pasarelas de pago,** garantizar la seguridad y la eficacia de las pasarelas de pago a través de la inversión en infraestructura y la capacitación de los usuarios contribuirá a una imagen más positiva y confiable de estas plataformas, esto aumentará la percepción de seguridad y confianza por parte de los usuarios.

- **Protección en la cadena de valor,** al minimizar las vulnerabilidades y mejorar la seguridad en las pasarelas de pago, se protege no solo a la empresa propietaria de la pasarela, sino a todos los actores involucrados en la cadena de valor, incluyendo a los proveedores, socios comerciales y clientes, asegurando transacciones más seguras en toda la red.

- **Incremento de la confianza de los usuarios en las compras online**, una experiencia de usuario más segura y satisfactoria fomentará la confianza de los usuarios en las compras en línea, disminuyendo la resistencia a utilizar pasarelas de pago, aumentando la disposición a realizar transacciones electrónicas con mayor frecuencia.

Todo lo anterior permite lograr el **Incremento de la confianza de los usuarios en las compras online.** El diagrama es un ejemplo de cómo las empresas pueden tomar medidas para reducir los incidentes de seguridad en las pasarelas de pago; al centrarse en la educación de los usuarios, la inversión en infraestructura y la mitigación de riesgos, las empresas pueden mejorar su seguridad y proteger a sus clientes de los ataques.

2.6 CUÁL ES LA SITUACIÓN DESEADA

En el entorno de las transacciones en línea dentro las pasarelas de pago, la seguridad emerge como una prioridad ineludible. Ante esta realidad, surge la necesidad de una autenticación más avanzada, dinámica, que ayude a garantizar la protección de la información de los usuarios y sus recursos económicos adoptándose proactivamente a las amenazas emergentes. Entre los desafíos más prominentes se encuentra la vulnerabilidad de los códigos de seguridad tradicionales, como el CVC estático, que ha dejado una puerta abierta a potenciales riesgos.

Para abordar este desafío, la implementación de un CVC dinámico, el código CVC de seguridad se actualiza automáticamente a intervalos regulares, proporcionando una autenticación dinámica que dificulta los intentos de fraude. Esta solución no solo refuerza la seguridad en las transacciones, sino que también ofrece la capacidad de detectar cualquier actividad no autorizada de inmediato, marcando un avance significativo en la protección de las transacciones en línea en el entorno digital actual.

Para lograr este propósito, además de fortalecer las medidas de seguridad técnicas, se ha definido la misión de educar al usuario, para que con el conocimiento adecuado y las herramientas necesarias puedan identificar situaciones de riesgo y

tomar acciones necesarias según el caso presentado, contribuyendo a reducir los incidentes de seguridad en las transacciones línea, garantizar el acceso a bienes y servicios en línea con plena confianza en la protección de sus datos y recursos económicos.

En la siguiente tabla se detalla una comparativa de la situación actual y cuál es la situación deseada de acuerdo con la solución propuesta.

Situación Actual	Situación Deseada
• Un panorama actual en el entorno digital colombiano muestra un desafío ante el incremento de los incidentes de seguridad en las transacciones en línea dentro de las pasarelas de pago. • Poca confianza de los usuarios en el uso de las pasarelas de pago. • Métodos de autenticación débiles, políticas de seguridad vulnerables e Insuficiente supervisión y monitoreo en tiempo real de las transacciones en línea.	• Se busca construir un entorno digital más seguro y confiable, a través de una solución Cloud mediante el desarrollo de un código CVC dinámico, que proporcione mayor seguridad al utilizar las pasarelas de pago y reducir los incidentes de seguridad en las transacciones en línea. • Usuarios capacitados para detectar situaciones de riesgos y amenazas cibernéticas, a través de cursos interactivos para utilizar correctamente las pasarelas de pago. • Mitigar riesgos y costos no proyectados tanto de las entidades bancarias como de los usuarios.

Tabla 1: Comparativa de la situación actual y situación deseada. Fuente de Elaboración: Propia.

2.7 INTRODUCCIÓN A LA SITUACIÓN DESEADA

En la última década, el crecimiento significativo de las transacciones online en Colombia ha impulsado la economía digital, pero no está exento de desafíos. La evolución tecnológica sido un catalizador para la economía digital brindando comodidad y accesibilidad a los consumidores, pero también ha dado lugar a preocupaciones significativas por vulnerabilidades considerables en términos de seguridad financiera y protección de datos.

El escenario actual en el entorno digital colombiano muestra un panorama desafiante por el incremento significativo de los incidentes de seguridad en línea, particularmente en el ámbito de las transacciones electrónicas generando una creciente preocupación. Las amenazas de fraude, la suplantación de identidad, las tácticas de ingeniería social y el phishing han aumento estos casos, convirtiéndose en problemas recurrentes que impactan la integridad de estas transacciones, comprometiendo la confianza de los usuarios en el entorno digital.

Los fraudes informáticos han sido un problema creciente en el país en los últimos años, en la siguiente gráfica se puede observar el reporte de fraudes en los últimos tres años.

“En la gráfica se presenta el número de denuncias reportadas por año y la respectiva variación porcentual por año de los ciberdelitos en Colombia los cuales han aumentado considerablemente en los últimos años. En 2022, el aumento fue del 28,8%, mientras que en lo que va de 2023, el aumento ha sido del 45,2%. Este aumento podría deberse a varios factores, como el aumento de la digitalización en Colombia, la mayor adopción de las tecnologías digitales y la sofisticación de los ciberdelincuentes.” [45]

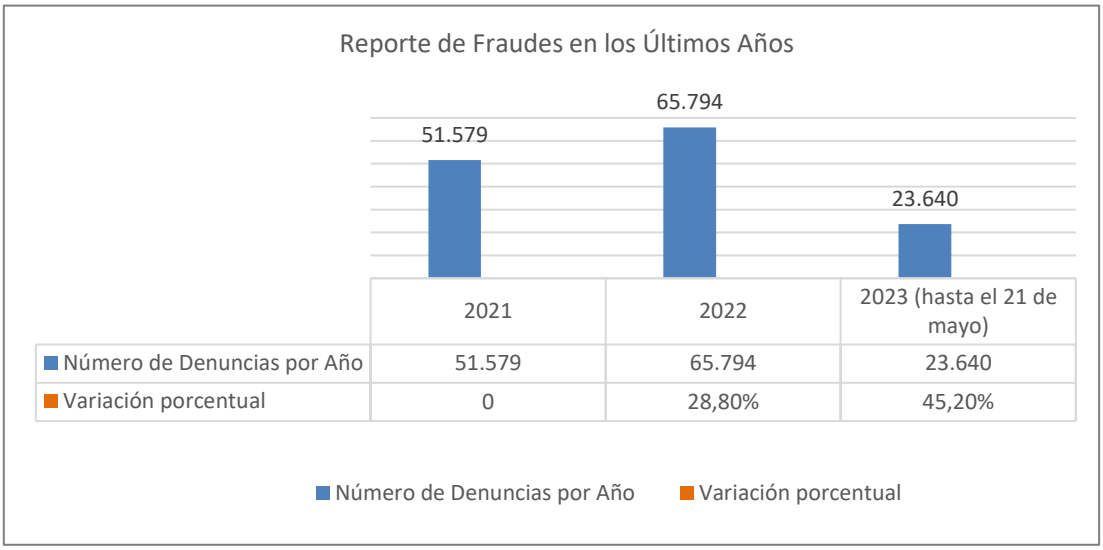

Figura 8. Situación actual Reporte de Fraudes Fuente: Elaboración propia.

De los fraudes reportados en los últimos años, en la siguiente gráfica se puede encontrar detallados los delitos informáticos más recurrentes reportados en el país. Los datos muestran que los delitos informáticos más reportados en Colombia son los que tienen un impacto económico, como el hurto por medios informáticos, violación de datos personales que representan el 23,5% del total de denuncias. Los delitos que tienen un impacto más disruptivo, como el acceso abusivo a sistemas informáticos y la suplantación de sitios web, representan el 9,2% del total de denuncias. El uso de software malicioso es un delito menos frecuente, pero que puede tener un impacto significativo, ya que puede provocar daños a los sistemas informáticos y la pérdida de datos.

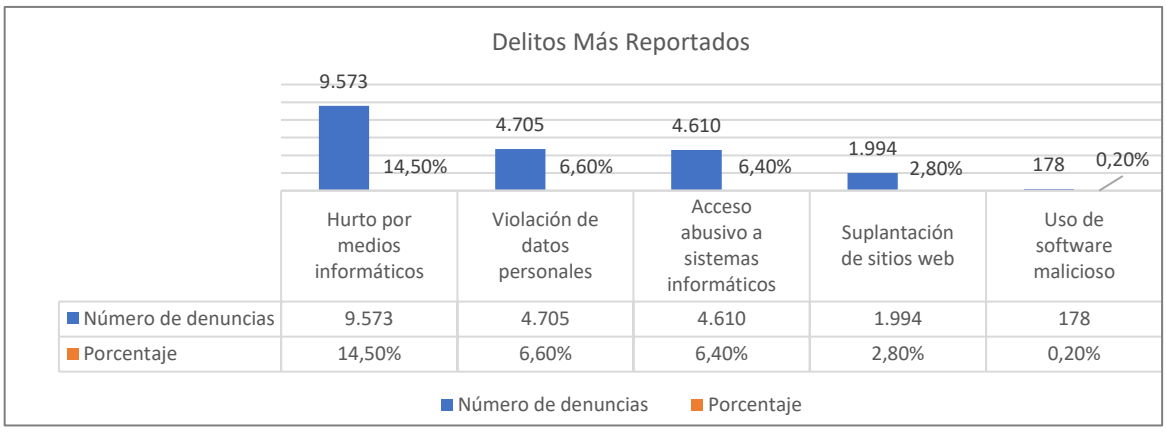

Figura 7. Delitos Más Reportados Fuente: Elaboración Propia

En este contexto, surge la necesidad imperiosa de trazar un camino hacia una mayor seguridad en línea. Por lo tanto, se proyecta una solución que involucre todos los aspectos de seguridad de la información de los usuarios y de las entidades, a través de nuevas tecnologías que se encuentran en tendencia como el Cloud, implementando mediante esta tecnología un código CVC dinámico que permita reducir los incidentes de seguridad en las transacciones online de las pasarelas de pago, para aumentar la confianza de los usuarios en las compras online.

En la siguiente gráfica podemos apreciar los beneficios más relevantes de adoptar un código CVC dinámico implementado a través de tecnologías Cloud.

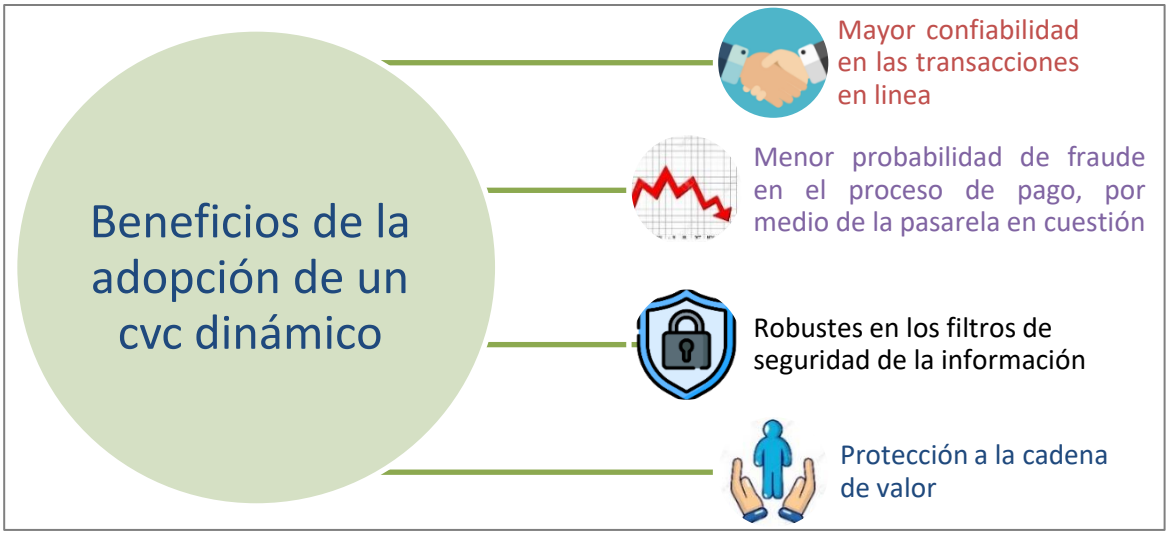

Figura 9. Gráfica situación Deseada Fuente: Elaboración propia.

Discriminando los beneficios de aplicar la solución planteada de un CVC dinámico se detalla:

Reducción de la reutilización de datos: Al utilizar un CVC dinámico, se minimiza la posibilidad de que los datos de la tarjeta sean reutilizados o almacenados, lo que disminuye el riesgo de exposición a posibles brechas de seguridad.

Aumento de la protección ante el robo de información: La implementación de un CVC dinámico añade una capa adicional de seguridad, lo que dificulta a los delincuentes el uso de información robada, ya que este código cambia regularmente y es válido solo por un corto período de tiempo.

Mejora de la experiencia del usuario: Aunque implica una capa de seguridad adicional, el proceso de introducir un CVC dinámico puede ser más conveniente para los usuarios que sistemas de verificación más complejos, lo que mejora su experiencia de compra en línea.

Cumplimiento normativo y estándares de seguridad: La adopción de un CVC dinámico puede ayudar a cumplir con los requisitos regulatorios y estándares de seguridad de la industria, lo que fortalece la posición de la empresa frente a posibles sanciones y mejora su reputación en términos de protección de datos.

2.8 PROPUESTA DE VALOR

Nuestra propuesta de valor se centra en brindar seguridad, confianza y educación en un entorno digital en constante evolución. El compromiso de reducir los incidentes de seguridad en línea, especialmente en las pasarelas de pago, asegurando que los datos de los usuarios y sus recursos económicos estén protegidos en cada transacción. Más allá de las medidas técnicas, nuestra misión es empoderar a los usuarios a través de la educación, proporcionando las herramientas y el conocimiento para que puedan identificar y mitigar situaciones de riesgo. Al elegir nuestra solución, los consumidores y las empresas pueden confiar en que sus interacciones en línea se basan en la seguridad, la integridad y la transparencia, garantizando una experiencia digital más segura y satisfactoria para todos.

2.8.1 Perfil Del Cliente

El cliente objetivo se dirige a instituciones financieras que proporcionan servicios mediante pasarelas de pago y reconocen la relevancia de resguardar la información de sus clientes y los activos financieros relacionados con estas pasarelas. Este cliente está en busca de una solución completa que no solo mejore las medidas técnicas de seguridad, sino que también ponga énfasis en la educación del usuario para establecer relaciones de confianza sólidas con su base de clientes. Se compromete a proporcionar un entorno digital seguro y confiable.

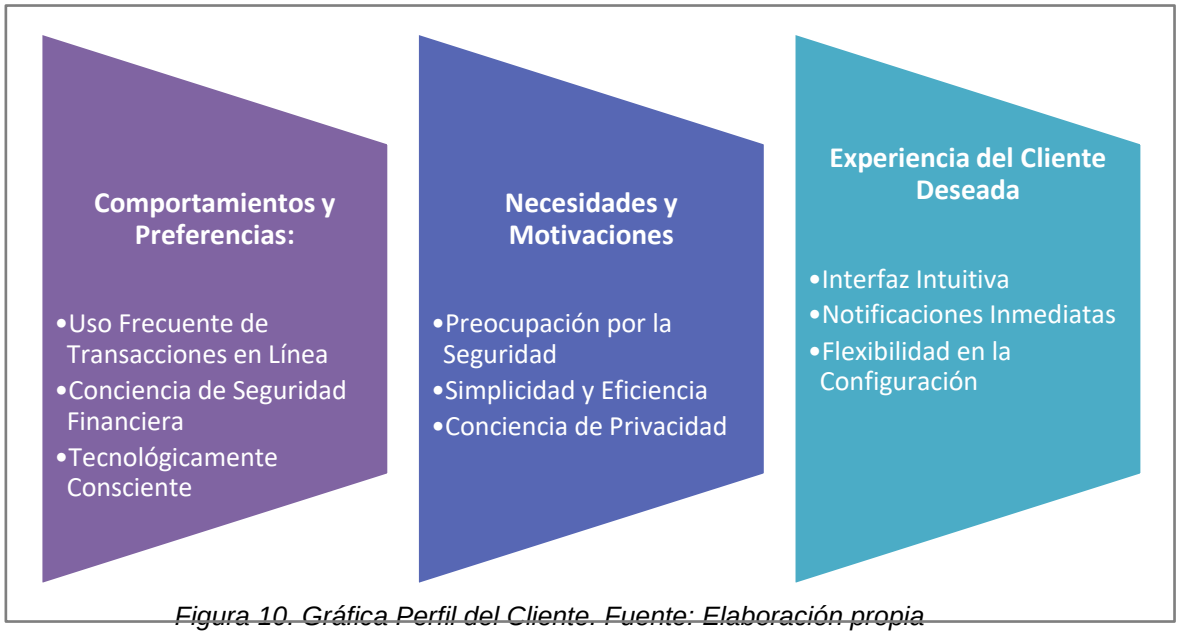

Figura 10. Gráfica Perfil del Cliente. Fuente: Elaboración propia

En el perfil del cliente se muestran las secciones de: comportamientos y preferencias, necesidades y motivaciones, y experiencia de la cliente deseada.

Comportamientos y preferencias: Se identifican las preferencias del cliente, es un usuario frecuente de transacciones en línea consciente de la seguridad financiera y es tecnológicamente consciente.

Necesidades y motivaciones: Se muestra que el cliente está preocupado por la seguridad, busca simplicidad y eficiencia, y es consciente de la privacidad.

Experiencia del cliente deseada: Se muestra que el cliente desea una interfaz intuitiva, notificaciones inmediatas y flexibilidad en la configuración.

En resumen, el cliente ideal para en esta propuesta es una entidad que busca no solo proteger sus operaciones en línea, sino también enriquecer la experiencia de usuario al ofrecer seguridad y educación, construyendo así una reputación sólida y generando confianza entre sus consumidores y socios comerciales.

2.8.2 Mapa De Valor

La propuesta planteada logra identificar que se puede mejorar los estándares de seguridad que actualmente se manejan en las transacciones a través de las pasarelas de pago, trazando un modelo de costo beneficio, tanto para las entidades bancarias, como los usuarios finales. A continuación, se evidencian los generadores de alegrías, producto propuesto y aliviadores en función de la solución propuesta.

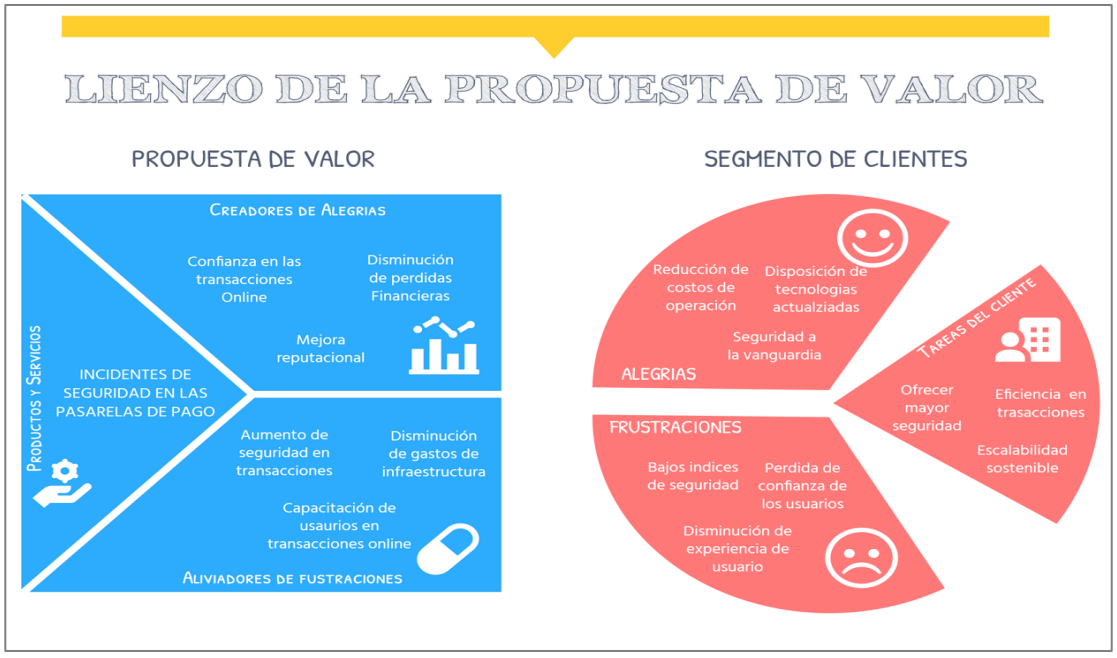

Figura 11. Propuesta de Valor. Fuente: Elaboración propia.

La representación visual de la propuesta de valor se divide en **Propuesta de valor** y **Segmento de clientes** donde se incluyen los aspectos más importantes de la estrategia planteada en la propuesta de valor. En la **Propuesta de valor** se detalla**:**

Creadores de alegrías: Este ítem pretende generar confianza a los usuarios al momento de realizar transacciones en línea, así mismo, generar seguridad para que el usuario pueda seguir utilizando este mecanismo de pagos con toda tranquilidad. Por otra parte, las entidades financieras mejorarán su reputación y las pérdidas económicas disminuirán.

Aliviadores de Frustraciones: Se contempla realizar capacitaciones y concientizaciones a los usuarios, con el fin de mitigar los ciberdelitos de este tipo, así mismo, se podrá contar con un nivel de seguridad más alto del lado del usuario y las entidades financieras realizaran inversiones menos costosas en términos de su infraestructura.

Productos y servicios: el producto y/o servicio que describe este documento, contempla funcionalidades de tipo dinámico, donde tanto los usuarios como las entidades financieras sentirán cierto alivio en función de las transacciones online, se pretende mitigar el riesgo de los delitos informáticos.

En el **Segmento de Clientes** se detalla:

Frustraciones: los usuarios de cierta manera sienten frustraciones al momento de realizar pagos online, esto debido a que las experiencias de usuario no son buenas, ya que en muchos casos se presenta fraude o perdidas de dinero, debido a la poca capacitación que puede tener un usuario en términos de ciberseguridad.

Alegrías: Con la implementación de soluciones tecnológicas que permitan a las entidades financieras reducir costos operacionales, se puede llegar a tener una

mejora reputacional, así mismo, realizar el acompañamiento a los usuarios para capacitarlos en temas de seguridad en transacciones en línea, de esta manera, se generan alegrías para las entidades y usuarios, donde vemos reducción de costos operaciones y reducción en fraudes informáticos.

Tareas del cliente: tal como se mencionaba anteriormente, con la implementación de soluciones tecnológicas que estén a la vanguardia, las entidades verán reflejadas las reducciones en costos de infraestructura, teniendo una escalabilidad de acuerdo al crecimiento de entidad, esto brindará mayor eficiencia en todos los procesos y una utilización de recursos optima.

2.8.3 Definición Propuesta de Valor

La situación actual, caracterizada por los desafíos crecientes en seguridad en línea busca lograr la reducción de incidentes de fraude y de seguridad en las transacciones electrónicas, se propone una solución a través de las tecnologías Cloud el desarrollo de un código CVC dinámico, que permita reducir los incidentes de seguridad en las transacciones en línea de las pasarelas de pago, con el fin de aumentar la confianza de los usuarios en las compras online. De esta manera de se busca construir un entorno digital más seguro y confiable, mitigando riesgos y costos no proyectados tanto de las entidades bancarias como de los usuarios.

2.9 PLANTEAMIENTO DE LA SOLUCIÓN

En el panorama digital actual, las transacciones son esenciales en la vida diaria. Sin embargo, esta creciente dependencia de la tecnología también ha traído consigo un aumento en los incidentes de seguridad en línea, lo que plantea desafíos significativos para la protección de datos y recursos económicos. En respuesta a esta creciente preocupación, hemos desarrollado un planteamiento de solución

integral para abordar y mitigar estos incidentes de seguridad en las transacciones en línea. Nuestra solución se basa en la combinación de medidas técnicas avanzadas, educación del usuario y un enfoque proactivo en la prevención de riesgos. A lo largo de esta propuesta, presentaremos en detalle cómo nuestra solución garantiza la seguridad y la confianza en las transacciones en línea, protegiendo los datos de los usuarios y sus recursos económicos de manera efectiva.

Para garantizar la autenticación del usuario antes de proporcionar información personal y sensible, se utiliza un código CVC dinámico. Este método ayuda a mantener la confidencialidad de los datos, protegiendo la información personal y bancaria al evitar compartirla con fuentes no verificadas. Además, es fundamental asegurar que la información no sea alterada o modificada de manera no autorizada, garantizando la integridad de los datos.

Es igualmente importante asegurar que las comunicaciones y transacciones en línea se realicen de manera segura, evitando la manipulación por parte de terceros malintencionados. Para ello, debemos garantizar que los servicios en línea estén disponibles cuando se necesiten, protegiéndolos contra malware y otros ataques que puedan afectar su disponibilidad. Adicionalmente, la conciencia de seguridad es uno de los pilares fundamentales. Es crucial estar informado sobre las últimas técnicas de fraude en línea, como el smishing, y comprender cómo protegerse para evitar caer en estas trampas.

Los planes educativos y preventivos en ciberseguridad buscan capacitar a emppleados y organizaciones para enfrentar ciberataques mediante talleres, seminarios, y material didáctico sobre prácticas seguras, como evitar enlaces y archivos sospechosos, y usar soluciones de seguridad actualizadas. Además, incluyen cursos de formación obligatorios, simulacros de ciberataques, políticas de

seguridad interna y auditorías regulares para empleados. Para transacciones en línea seguras, se recomienda verificar la autenticidad de los sitios de pago, asegurar conexiones seguras, preferir comercios reconocidos y emplear autenticación multifactor, manteniendo siempre la conciencia de seguridad y actualización sobre técnicas de fraude. Implementar estos planes educativos y preventivos ayudará a mejorar la ciberseguridad tanto a nivel individual como organizacional, y protegerá a los usuarios durante las transacciones en línea. La educación continua y la adopción de prácticas seguras son esenciales para mitigar los riesgos cibernéticos en el entorno digital actual.

2.9.1 Análisis de solución

Teniendo en cuenta que la solución propuesta involucra tecnologías cloud, se contempla el uso de algunos servicios que ofrece Amazon Web Services (AWS), con el fin de tener un proyecto bien estructurado y escalable en el tiempo, hablando en términos de los componentes técnicos. AWS como uno de los grandes proveedores de nube, ofrece precios atractivos bajo el principio de pago por uso, lo que viabiliza realizar implementaciones de servicios en esta tecnología.

De acuerdo con la definición del proveedor a utilizar, se propone una arquitectura que contemple el menor costo posible, así mismo, que genere el menor impacto en los usuarios y las entidades financieras.

En pro de resaltar los 3 pilares importantes de la seguridad de la información (confidencialidad, integridad y disponibilidad), se propone la implementación de un componente de software que permita la generación de códigos CVC que cambien aleatoriamente en un periodo de tiempo corto o en cada compra que se vaya a realizar de manera Online, este código será notificado al usuario a través de los

diferentes métodos de contacto que previamente se configuran (Correo electrónico, SMS, llamada o WhatsApp), el método también será aleatorio de acuerdo a lo que se encuentre a disposición.

Posible Solución	Deseable	Viable	Factible	Sostenible
Reconocimiento Facial en tiempo real	Si	Tal vez	Si	Si
Generación de CVC dinámico	Si	Si	Si	Si

Tabla 2: Posibles soluciones. Fuente de Elaboración: Propia.

2.9.2 Identificación de tecnologías

Dentro de las opciones al implementar soluciones tecnológicas las tecnologías Cloud tienen muchos beneficios debido a la facilidad y rapidez de escalar horizontal y verticalmente, también por su gran beneficio de operar bajo el modelo de pago por uso. Teniendo en cuenta que AWS podrá suplir la necesidad para el diseño e implementación de una arquitectura que soporte el componente de software para la generación de códigos CVC aleatorios, se procederá con el uso de los siguientes servicios que ofrece la plataforma:

- **Amazon API Gateway.**
- **Amazon Lambda.**
- **Amazon DynamoDB.**
- **Amazon Relational Database Service (RDS).**
- **Amazon Simple Notification Service (SNS).**
- **Amazon CloudWatch.**

3 ANÁLISIS DE LAS ALTERNATIVAS TÉCNICAS PARA SOLUCIONAR EL PROBLEMA

Una de las mejores opciones en cuanto implementaciones de soluciones tecnológicas hoy en día, es el Cloud, debido a la facilidad y rapidez de escalar horizontal y verticalmente, también por su gran beneficio de operar bajo el modelo de pago por uso. Teniendo en cuenta que AWS podrá suplir la necesidad para el diseño e implementación de una arquitectura que soporte el componente de software para la generación de códigos CVC aleatorios, se procederá con el uso de los siguientes servicios que ofrece la plataforma:

3.1 AMAZON API GATEWAY:

“Amazon API Gateway es un servicio completamente gestionado que simplifica la tarea de los desarrolladores de construir, publicar, mantener, supervisar y proteger API en cualquier escala. Las API funcionan como la "entrada" que permite a las aplicaciones acceder a los datos, lógica empresarial o funciones de servicios en la parte posterior. Con API Gateway, es posible crear API RESTful y API WebSocket que posibilitan la comunicación en tiempo real bidireccional para las aplicaciones. Además, API Gateway es compatible con cargas de trabajo basadas en contenedores, sin servidor y aplicaciones web.” [46]

3.2 AMAZON LAMBDA:

“AWS Lambda es un servicio informático sin servidor y basado en eventos que posibilita la ejecución de código para una amplia variedad de aplicaciones o servicios en la parte posterior, sin la necesidad de configurar o gestionar servidores. Puede activar Lambda desde una amplia gama de servicios de AWS y aplicaciones de software como servicio (SaaS) y, lo mejor, solo paga por el uso que le da.” [47]

3.3 AMAZON DYNAMODB:

“Amazon DynamoDB es una base de datos NoSQL de clave-valor sin servidor y completamente administrada que está diseñada para ejecutar aplicaciones de alto rendimiento a cualquier escala. DynamoDB ofrece seguridad integrada, copias de seguridad continuas, replicación automatizada en varias regiones, almacenamiento de caché en memoria y herramientas de importación y exportación de datos.” [48]

3.4 AMAZON RELATIONAL DATABASE SERVICE (RDS):

“Amazon Relational Database Service (Amazon RDS) es un conjunto de servicios gestionados que simplifican la configuración, operación y expansión de bases de datos en la nube. Puede seleccionar entre siete motores de bases de datos populares, que incluyen Amazon Aurora con compatibilidad para MySQL, Amazon Aurora con compatibilidad para PostgreSQL, MySQL, MariaDB, PostgreSQL, Oracle y SQL Server, y también desplegarlo en las instalaciones mediante Amazon RDS en AWS Outposts.” [49]

3.5 AMAZON SIMPLE NOTIFICATION SERVICE (SNS):

“Amazon Simple Notification Service (Amazon SNS) ofrece dos métodos de envío de notificaciones: A2A y A2P. A2A permite la entrega de mensajes basada en push de alto rendimiento, de uno a muchos, entre sistemas distribuidos, microservicios y aplicaciones sin servidor que funcionan con eventos. Estas aplicaciones incluyen Amazon Simple Queue Service (SQS), Amazon Kinesis Data Firehose, AWS Lambda y otros puntos de conexión HTTPS. Por otro lado, la función A2P le capacita para enviar mensajes a sus clientes a través de SMS, notificaciones push y correos electrónicos.” [50]

3.6 AMAZON CLOUDWATCH:

"Amazon CloudWatch recopila y presenta en paneles automatizados los registros, métricas y datos de eventos en tiempo real, lo que simplifica la gestión y el mantenimiento de la infraestructura y las aplicaciones." [51]

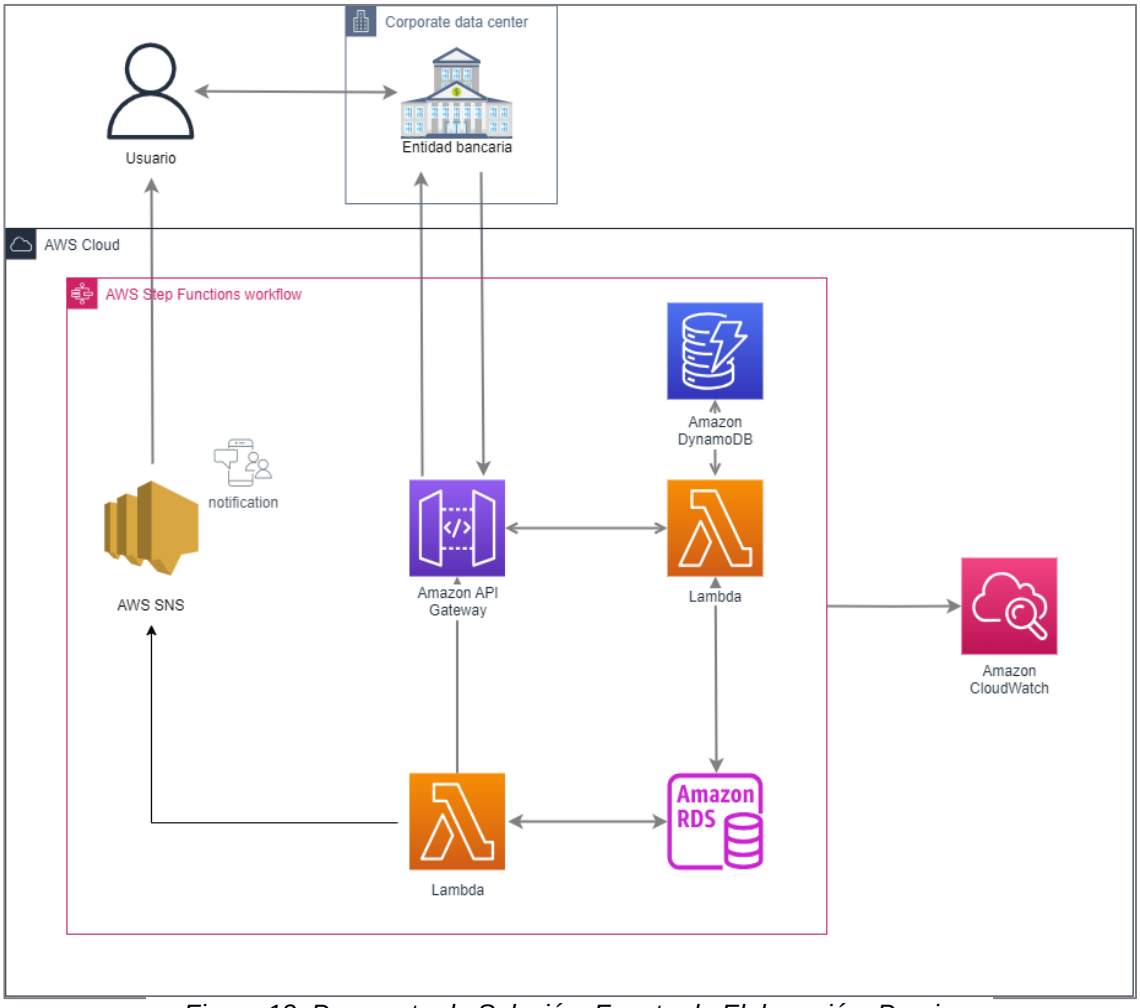

Figura 12. Propuesta de Solución. Fuente de Elaboración: Propia

La aplicación bancaria implementa un proceso de seguridad adicional al requerir que los usuarios ingresen el código CVC generado específicamente para cada transacción al ingresar los datos de la tarjeta en las pasarelas de pago. Este código, con una validez temporal definida, se proporcionará a través de la aplicación y será utilizado únicamente para esa transacción en particular. Posteriormente, el código

se invalidará automáticamente para garantizar la seguridad de la información financiera de los usuarios, minimizando así el riesgo de posibles vulnerabilidades o usos no autorizados.

3.7 RESPALDO EN NUBE MICROSOFT AZURE

Como medida de contingencia ante eventos no planificados sobre el servicio de AWS, se proyecta una segunda arquitectura para el servicio de generación de códigos CVC, haciendo uso de algunos de los componentes de la nube de Microsoft Azure:

3.7.1 Azure Notification Hubs:

“Representa un sistema escalable de envío masivo de notificaciones móviles que posibilita el rápido envío de un gran volumen de notificaciones a dispositivos iOS, Android, Windows o Kindle, compatibles con servicios como APNs (Apple Push Notification Service), GCM (Google Cloud Messaging), WNS (Windows Push Notification Service), entre otros. Esta herramienta permite personalizar las notificaciones para clientes individuales o audiencias completas con una mínima cantidad de código, siendo compatible con diversas plataformas para su implementación.” [52]

3.7.2 Azure Functions:

“Esta plataforma presenta el procesamiento sin servidor impulsada por eventos, diseñada para facilitar un desarrollo más eficiente con la flexibilidad de utilizar el lenguaje de programación preferido por el usuario. Esta solución permite enfocarse en la lógica principal del negocio, proporcionando el máximo nivel de abstracción del hardware y simplificando así la gestión y optimización de recursos.” [53]

3.7.3 Azure API Management:

“Despliega múltiples puertas de enlace de API de manera simultánea para conectarte con APIs alojadas en Azure, diferentes plataformas en la nube y en entornos locales, con el objetivo de mejorar y agilizar el tráfico entre estas APIs. Cumple con los estándares de seguridad y regulaciones requeridas, al tiempo que experimentas una gestión unificada y una visibilidad total de todas las APIs, tanto internas como externas, para una observación completa de su funcionamiento.” [54]

3.7.4 Azure Cosmos DB:

“Creación ágil y adaptable de aplicaciones mediante oportunidades de desarrollo y pruebas sin costo, diversidad de Kits de Desarrollo de Software (SDK), y soporte para bases de datos de código abierto como PostgreSQL, MongoDB y Apache Cassandra.” [55]

3.7.5 Azure SQL Database:

“Es un servicio de base de datos relacional completamente gestionado y constantemente actualizado, específicamente diseñado para el entorno en la nube. Facilita el desarrollo de aplicaciones aprovechando la versatilidad de una base de datos con múltiples modelos, escalable para adaptarse a las necesidades de uso, permite el análisis en tiempo real sin comprometer el rendimiento gracias a Azure Synapse Link para SQL Database.” [56]

3.7.6 Azure Monitor:

“Facilita la gestión de sus operaciones a gran escala, al optimizar el rendimiento y la disponibilidad de los recursos, además de detectar anticipadamente posibles problemas. Permite recopilar, analizar y tomar acciones basadas en la información de telemetría proveniente de entornos tanto híbridos como en la nube.” [57]

En la Figura 13 se presenta detalladamente la arquitectura establecida como una precaución ante posibles eventos inesperados que puedan afectar el servicio de AWS. Como una medida adicional de contingencia para el sistema de generación de códigos CVC, se ha diseñado una segunda arquitectura aprovechando ciertos elementos disponibles en la plataforma de Microsoft Azure en caso de fallos o interrupciones en AWS.

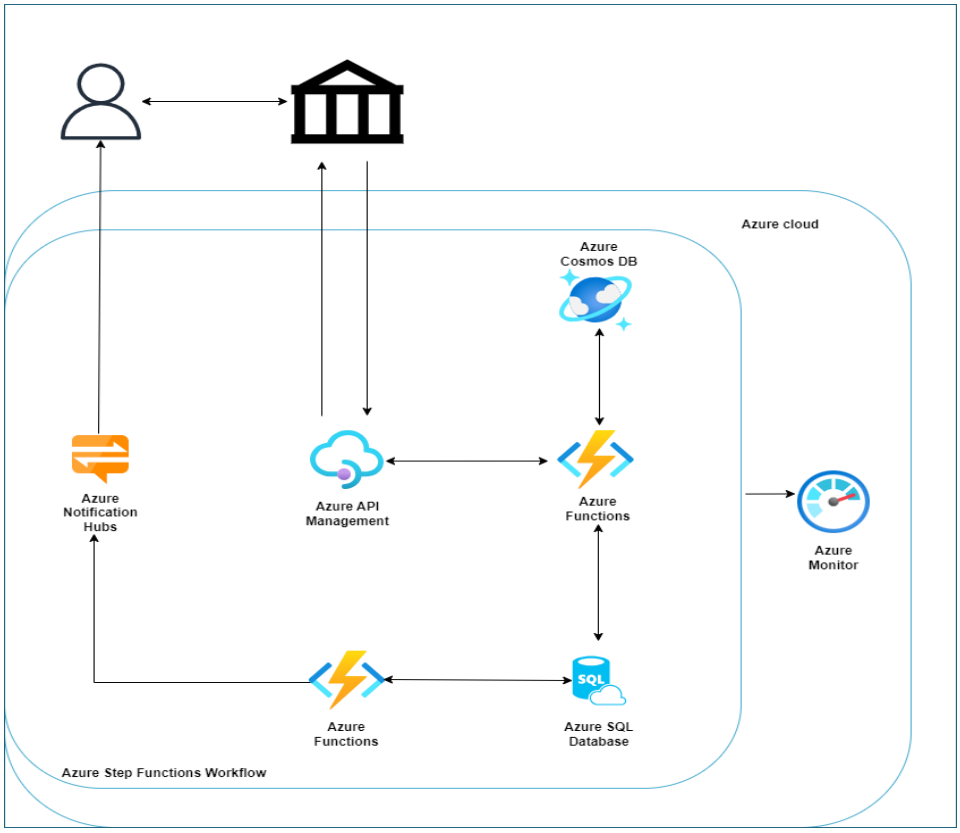

Figura 13. Propuesta de Solución (Respaldo). Fuente de Elaboración: Propia

En las dos arquitecturas presentadas sobre la nube de AWS y Microsoft Azure servicios que notificaran a los usuarios a través de los diferentes medios que se pueda disponer el usuario (SMS, Email, push), así mismo, se utilizan servicio de tipo Serverless con el fin de ejecutar las funciones que permitirá la generación de los

códigos CVC, este tipo de transacciones serán almacenadas en bases de datos NoSQL y SQL, para guardar toda la traza y log que da como resultado la ejecución de las funciones, por último, la arquitectura será supervisada por un servicio de monitoreo, para validar que todos los servicios se encuentre en línea y no genere algún tipo de indisponibilidad.

Para abordar los desafíos de seguridad asociados con la generación de códigos CVC para transacciones bancarias en línea, los servicios específicos de AWS y Azure proporcionan herramientas robustas que mitigan posibles amenazas como el acceso no autorizado o la manipulación de datos. Estas herramientas permiten implementar medidas de seguridad en cada etapa del proceso, desde la generación de códigos CVC hasta el almacenamiento de datos en las bases de datos, para proteger la información confidencial de los usuarios y garantizar la integridad de la aplicación. Al integrar estos servicios de seguridad de manera efectiva, una aplicación bancaria puede mejorar significativamente su resistencia a las amenazas cibernéticas, protegiendo tanto los datos sensibles de los clientes como la reputación de la institución financiera.

Los servicios de AWS y Microsoft Azure, como AWS Lambda, Amazon S3, AWS IAM, Amazon RDS, AWS CloudWatch, Azure Functions, Azure Notification Hubs, Azure Cosmos DB, Azure SQL Database y Azure Monitor, contribuyen a mitigar posibles amenazas, como el acceso no autorizado o la manipulación de datos, al proporcionar una infraestructura segura, altamente escalable y con capacidad para cumplir con los estándares de seguridad de la industria.

La integración de estos servicios en la infraestructura existente de la aplicación bancaria garantiza una gestión centralizada y efectiva de los recursos, facilitando la detección y respuesta proactiva ante posibles incidentes de seguridad. Estos servicios permiten implementar medidas de seguridad avanzadas, como controles de acceso granular, cifrado de datos, monitoreo continuo, alertas y notificaciones en

tiempo real, y auditorías exhaustivas. Esto asegura la protección de la información financiera de los usuarios y la integridad de la aplicación bancaria. Todo esto contribuye a establecer un entorno sólido ante posibles amenazas y vulnerabilidades de seguridad.

A continuación, se explica cómo estos servicios contribuyen a la seguridad y cómo se integrarían en la infraestructura existente de la aplicación bancaria, con ejemplos específicos de implementación.

- Utilización de AWS IAM y Azure Active Directory para gestionar de forma segura los permisos de acceso a los servicios en la nube, asegurando que solo usuarios autorizados puedan interactuar con los recursos.
- Almacenamiento cifrado de los códigos CVC generados en Amazon S3 y Azure Cosmos DB para proteger la información confidencial de los usuarios.
- Implementación de AWS Lambda Functions y Azure Functions para ejecutar de forma segura y eficiente la generación de los códigos CVC, minimizando la exposición de código y reduciendo la superficie de ataque.
- Configuración de alertas y notificaciones en AWS CloudWatch y Azure Monitor para monitorizar de manera continua la actividad del sistema y detectar posibles anomalías o intentos de acceso no autorizado.
- Registro detallado de todas las transacciones y operaciones realizadas en Amazon RDS y Azure SQL Database, facilitando la trazabilidad y auditoría de los códigos CVC generados y garantizando la integridad de los datos.

Al implementar estos servicios de manera integrada en la infraestructura de la aplicación bancaria, se establece un entorno sólido de seguridad que protege los códigos CVC generados, garantizando la confidencialidad de la información, la autenticación adecuada de los usuarios y la integridad de los datos.

Las soluciones existentes suelen depender de infraestructuras locales o privadas, lo que puede generar limitaciones en escalabilidad, redundancia y seguridad. Además, su mantenimiento y actualización pueden resultar costosos y laboriosos. En contraste, las soluciones basadas en servicios en la nube como AWS y Microsoft Azure ofrecen una mayor flexibilidad, escalabilidad, seguridad y confiabilidad en comparación con las soluciones locales tradicionales. Algunas diferencias clave incluyen:

Escalabilidad: AWS y Azure permiten escalar fácilmente los recursos según la demanda, lo que garantiza un rendimiento óptimo en todo momento. Las soluciones locales pueden tener limitaciones en términos de capacidad y escalabilidad.

Seguridad: Los proveedores de servicios en la nube como AWS y Azure cuentan con medidas de seguridad avanzadas, como encriptación de datos, monitoreo continuo, autenticación multifactor y cumplimiento de estándares de seguridad de la industria. Esto proporciona una capa adicional de protección para los datos sensibles, como los códigos CVC generados.

Mantenimiento y actualizaciones: En la nube, los proveedores se encargan del mantenimiento de la infraestructura, las actualizaciones de software y la gestión de la seguridad, lo que reduce la carga operativa para el equipo de TI. En cambio, con una solución local, el mantenimiento y las actualizaciones pueden requerir recursos adicionales y tiempo.

En resumen, las soluciones basadas en servicios en la nube como AWS y Azure ofrecen una serie de ventajas en términos de escalabilidad, seguridad y facilidad de mantenimiento en comparación con las soluciones locales tradicionales, lo que las convierte en una opción atractiva para garantizar la seguridad y la integridad de los códigos CVC generados en una aplicación bancaria.

4 MODELO DE NEGOCIO

4.1 PROPUESTA DE MODELO DE NEGOCIO

El modelo de negocio de la solución propuesta, va enfocada a generar confianza a los usuarios en las transacciones que realizan en línea a través de las pasarelas de pago, dicha solución implementada con tecnología nube, busca que tanto los clientes como los administradores del servicio paguen únicamente por lo que usan, es decir, los clientes pagan por cada transacción realizada en línea donde se haga el llamado al servicio y los administradores, dueños de la aplicación, pago por el uso de los recursos informáticos que soportaran el servicio de generación de códigos CVC aleatorios.

Con el fin de tener una alta optimización de costos y fiabilidad de los servicios informáticos para las partes involucradas, se utilizarán los servicios de nube ofertados por Amazon Web Services o Microsoft Azure, aprovechando todas la bondades ofrecidas por este tipo de servicio, como por ejemplo, escalar servidores horizontal y verticalmente de acuerdo a la demanda de peticiones y así pagar únicamente por lo que se usa, esto permitirá que los costos de operación sean bajos y únicamente por los recursos que se usan, de esa manera se puede llegar a buscar eficiencia en costos, operación y servicio.

De acuerdo con lo anterior, la nube permite mantenernos a la vanguardia tecnológica en el sentido de utilizar tecnologías en tendencias que ayuden a impulsar el modelo de negocio de la solución propuesta.

Figura 14. Cuadrante Mágico de Gartner. Fuente de Elaboración: Gartner

4.2 VALIDACIÓN DEL MODELO DE NEGOCIO

Para la validación del modelo de negocio, se ha desarrollado el lienzo del modelo Canvas, el cual nos permite visualizar la propuesta de valor del negocio, así como los demás componentes que lo involucran, tales como: socios clave, actividades clave, relación con el cliente, costos, canales, fuentes de ingreso:

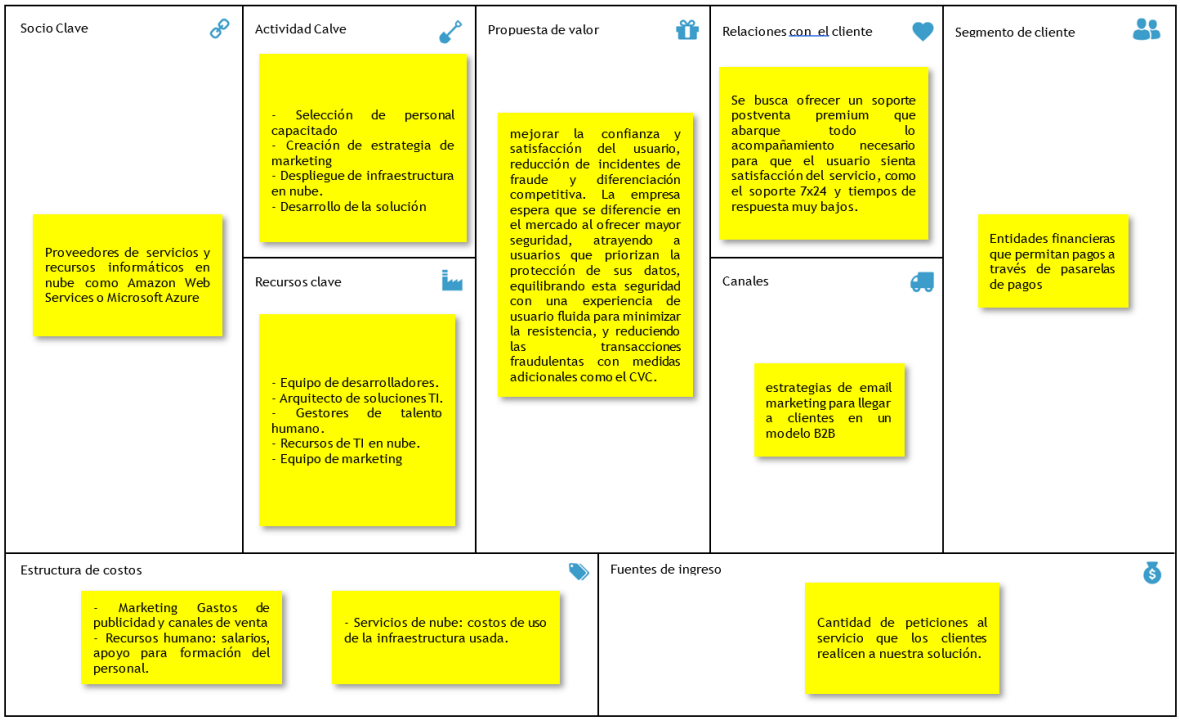

Figura 15. Lienzo del modelo Canvas para la solución propuesta. Fuente de Elaboración: Elaboración Propia.

Con el fin de dar una segunda validación de nuestro modelo de negocio nos basamos en estadísticas que nos dan información acerca del fraude en comercio electrónico en países como estados unidos, en al siguiente grafica evidenciamos como la gráfica ha venido aumentando en función del tiempo:

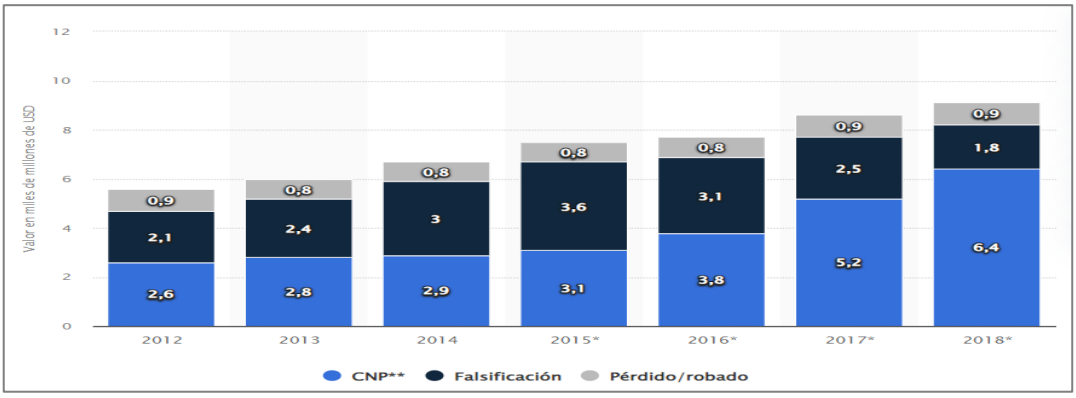

Figura 16. Evolución anual del valor de las pérdidas por fraude de tarjetas de pago en Estados Unidos desde 2012 hasta 2018, según el tipo de fraude. Fuente: Statista Research Department.

“La pandemia de COVID-19 ha acelerado el cambio al e-commerce, lo que ha provocado un aumento del 20 % de los valores de las transacciones en línea. Los confinamientos y las medidas de distancia social que se impusieron en 2020 obligaron a cerrar a muchos comercios físicos. Esto ha generado un aumento de la actividad del e-commerce, a raíz de que los consumidores eligiesen las compras por Internet por considerarlas una alternativa más segura y cómoda. En consecuencia, el e-commerce experimentó un crecimiento drástico durante la pandemia, con un incremento del 20 % de los valores de las transacciones en línea.” [58]

“Si bien este canal ha servido de salvavidas para algunas empresas que, sin él, habrían tenido que cerrar, provoca nuevos desafíos y riesgos para las organizaciones, que han de gestionar el peligro creciente del fraude de pagos y otras amenazas para la seguridad.” [59]

“Por otra parte, con el avance tecnológico, el modo de operación de los ciberdelincuentes también cambia, ya que estos inescrupulosos aprovechas las bondades de estas nuevas tecnológicas como lo es la Inteligencia Artificial, para mejorar sus técnicas para el fraude, ese sentido, se prevé que el coste del fraude de pagos en línea en todo el mundo pase de 130.000 millones de dólares en 2020 a 206.000 millones de dólares en 2025.” [60]

5 PROPUESTA DE LA SOLUCIÓN TECNOLÓGICA

Para mitigar los incidentes de seguridad en las pasarelas de pago, se propone el desarrollo de servicio que permita generar códigos CVC aleatorios que vayan asociadas a las tarjetas de crédito y débito de las entidades financieras, que serán necesarios a la hora de realizar compras online.

Este servicio se propone alojar en Cloud, con el fin de tener escalabilidad y disponibilidad, así mismo, con programación se busca que la información viaje encriptada para añadir capas de seguridad a los datos que se consuman de las entidades financieras.

En la actualidad realizar una compra online basta con tener el plástico o tarjeta de crédito/débito y la cédula de una persona. De acuerdo con lo anterior, no existe seguridad para validar que en realidad el dueño de dichas tarjetas es quien está realizando la compra, y es por eso que se propone agregar una capa de seguridad que permita mitigar estos incidentes de seguridad.

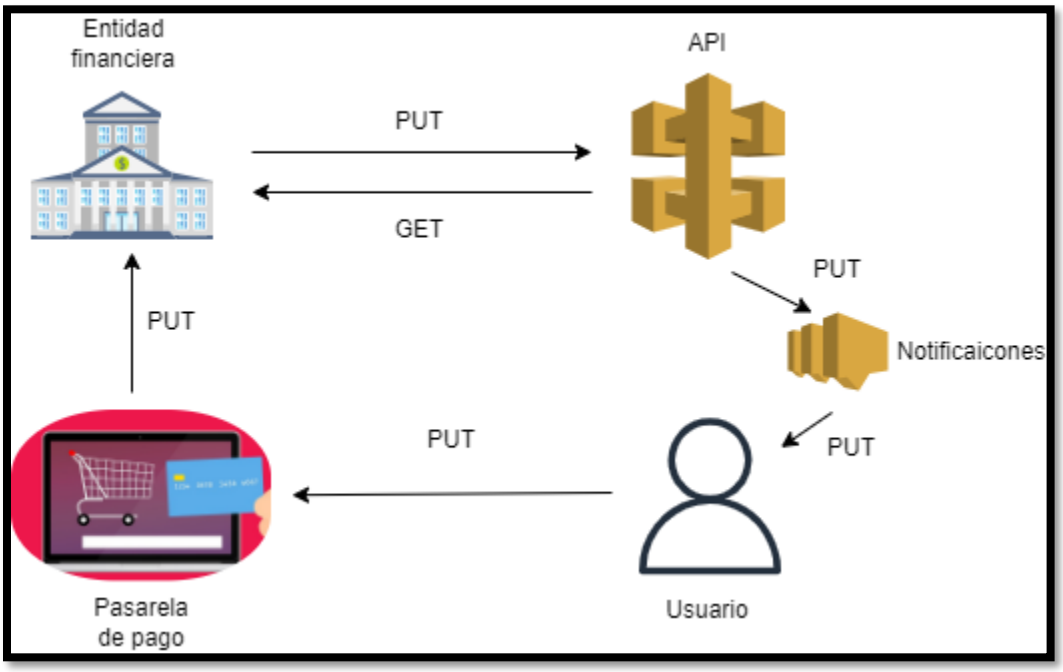

Figura 17 Funcionamiento De La Solución Propuesta. Fuente de Elaboración: Propia

El funcionamiento del servicio parte desde los principios de uso de API's (Application programming interface), ya que son mecanismos que permiten a dos componentes de software comunicarse entre sí mediante un conjunto de definiciones y protocolos. [61]; para este planteamiento se buscará la comunicación entre las entidades financieras y el servicio propuesto con el fin de generar un CVC aleatorio, asociado

a las tarjetas de crédito y débito para así añadir una capa de seguridad en las compras online.

La elección de implementar la solución en cloud, obedece a las bondades que se tienen allí, tales como la escalabilidad, agilidad y la economía en escala que se puede llegar a tener, principalmente se realizará la implementación en AWS, teniendo cuenta que según Gartnert, este proveedor es uno de los líderes en el mercado que ofrece infraestructura cloud, así mismo, esta cuenta con una gran variedad de servicios que nos ayudaría a suplir las necesidades para la puesta en marcha de la solución.

Con la implementación de la solución, se busca que, al momento de realizar alguna transacción en línea, se pueda ejecutar el servicio que genera códigos CVC aleatorios, y que este sea recepcionado por el usuario a través de mensaje de texto, llamada o correo electrónico, esto permitirá de cierto modo validar la identidad del usuario y evitar posibles estafas.

6 ANÁLISIS DEL PROCESO DE TRANSFORMACIÓN DIGITAL

La solución propuesta para mitigar los incidentes de seguridad en las pasarelas de pago, abarca 2 de los 5 pilares de la transformación digital, Cloud y Ciberseguridad, estos dos componentes importantes convergen para mejorar la experiencia del cliente al momento de realizar transacciones online.

“La tecnología Cloud ha revolucionado la manera en que desplegamos servicios de informática, brindándonos agilidad, escalabilidad y economía. De acuerdo con Gartnert, Amazon Web Services y Microsoft se muestran como los lideres en el mercado que ofrece este tipo de tecnología y es por ello se toma el camino de

implementar nuestra solución utilizando los servicios ofrecidos por AWS y Azure.” [62]

Figura 18. Cuadrante mágico de Gartnert Fuente de Elaboración: Gartnert

De acuerdo a los principios fundamentales de la transformación digital (Personas y cultura, experiencia del cliente, procesos y tecnología), la implementación de tecnologías como el Cloud y Ciberseguridad puede llegar a ser una limitante cuando no tenemos una cultura resiliente en nuestro entorno, para ello se debe contar con procesos que estén alienados a las nuevas tecnologías que se ajusten a nuestro modelo de negocio, esto permitirá que la transformación digital que implementemos sea más sencilla de adoptar y empecemos con la creación de cultura en las personas de manera escalar.

“En todos los sectores, las organizaciones están acelerando la transformación digital para lograr crecimiento y rentabilidad a largo plazo. Desde la perspectiva de

Gartner, “el viaje de transformación está llevando a las grandes empresas, especialmente, al menos el doble de tiempo y costando el doble de lo que anticiparon originalmente”. En gran parte, esto se debe a la preparación cultural: “el 53% de las organizaciones encuestadas aún no han sido probadas frente al desafío digital y, por lo tanto, su preparación para la transformación digital es incierta”.” [63]

A continuación, se destacan algunos hitos clave y una muestra de los recursos asociados de Gartner:

- Ambición: Estrategia definida e interés y entusiasmo generados.
- Diseñar: Opciones y ecosistema evaluados para el desarrollo del plan.
- Entregar: Prueba de concepto mínima viable ejecutada y comunicada.
- Escalar: Aclare cómo cambiará su gobernanza en comparación con los modelos actuales para reflejar las necesidades únicas de sus iniciativas específicas.
- Refinar: Evaluación, optimización y reevaluación.

7 ASPECTOS LEGALES Y CONTRATACIÓN

7.1 ASPECTOS DE REGULACIÓN:

7.1.1 Regulación de protección de datos:

Según la regulación de datos colombiana establecida en el 2012 reglamentada en la ley 1581 de 2012, la cual regula el tratamiento de datos, en específico el derecho que tienen las personas que se encuentren en el país, de conocer, actualizar y rectificar la información recopilada en las bases de datos, de cualquier sistema

público o privado según se requiera; tomando en cuenta excepciones relacionadas con la defensa nacional o bases de datos personales o de pruebas.

En el año 2013 se generó un decreto que reglamente o le adhiere condiciones a la ley 1581 de 2012, en donde se priorizan o resaltan puntos como, tratamiento de datos, políticas de tratamiento, derechos de los titulares, Transferencia de datos y rendición de cuentas. [64]

7.1.2 Regulación financiera y de seguridad:

Tomando en cuenta que los datos que se van que intervienen en la herramienta son datos de índole bancarios, se toman en cuenta datos de regulaciones financieras y de seguridad:

- **Circular Básica Jurídica (C.E. 029/14)**: Emitida por la Superintendencia Financiera de Colombia, esta circular establece instrucciones generales aplicables a las entidades vigiladas. [65]

- **Estándares Internacionales Aplicables**:

✓ **PCI DSS (Payment Card Industry Data Security Standard)**: Este estándar se utiliza para proteger la información de tarjetas de crédito y débito. Las empresas que procesan pagos deben cumplir con estas regulaciones para garantizar la seguridad de los datos de los titulares de tarjetas. [66]

✓ **ISO/IEC 27001**: Es una norma internacional para la gestión de la seguridad de la información. Muchas empresas en Colombia adoptan y adaptan esta norma para proteger sus sistemas y datos. [67]

7.2 CONTRATOS Y ACUERDOS

Tomando en cuenta la normativa que aplica Colombia bajo requerimiento de los contratos que se pueden suscribir, se toman como referencia en el marco normativo nacional e internacional los siguientes términos y condiciones:

- **Términos de Servicio y Políticas de Privacidad**: Deben estar alineados con la Ley 1581 de 2012 y el Decreto 1377 de 2013.
- **Acuerdos de Nivel de Servicio (SLA)**: Definen los niveles de servicio esperados y las responsabilidades de las partes.
- **Acuerdos de Procesamiento de Datos (DPA)**: Contratos específicos con terceros que procesen datos en tu nombre, asegurando el cumplimiento de la Ley 1581 de 2012. [64]

7.3 ASPECTOS CONTRACTUALES

Tomando como referencia la naturaleza del desarrollo, y de la puesta en marcha de la funcionalidad, se individualizan las características según la normativa nacional que se deben tener en cuenta en el momento de efectuar un proceso de contratación:

7.3.1 Selección de Proveedores:

- **Evaluación de Proveedores**: Realizar una evaluación exhaustiva de proveedores y socios tecnológicos para asegurar el cumplimiento con los estándares de seguridad y legales aplicables en Colombia.

- **Certificaciones de Seguridad**: Preferir proveedores que cuenten con certificaciones relevantes como ISO/IEC 27001 y PCI DSS. [67]

7.3.2 Cláusulas Contractuales:

- **Confidencialidad**: Incluir cláusulas de confidencialidad para proteger la información sensible.
- **Responsabilidad y Seguro**: Definir claramente la responsabilidad en caso de incumplimientos de seguridad y considerar incluir cláusulas de seguro.
- **Derechos de Propiedad Intelectual**: Establecer quién posee los derechos sobre el software y los datos generados. [65]

7.4 GESTIÓN DE RIESGOS

- ✓ **Auditorías y Evaluaciones Regulares**: Incluir cláusulas que permitan auditorías y evaluaciones de seguridad periódicas.
- ✓ **Plan de Respuesta a Incidentes**: Definir los procedimientos a seguir en caso de una brecha de seguridad. [65]

CONCLUSIONES

En un mundo cada vez más interconectado y dependiente de las transacciones en línea, la seguridad de los datos financieros se ha convertido en un tema crucial. Esta discusión ha presentado una propuesta integral centrada en abordar los desafíos de seguridad en las pasarelas de pago, combinando medidas técnicas avanzadas con una fuerte iniciativa educativa para usuarios y entidades financieras. La implementación de un sistema de generación de códigos CVC dinámicos ha surgido como una solución clave para fortalecer la protección de datos financieros y reducir los riesgos asociados con las transacciones electrónicas.

La propuesta destacó la importancia de comprender las necesidades y preferencias del cliente objetivo, principalmente instituciones financieras comprometidas con la seguridad y la confianza de sus clientes. Se resaltó la relevancia de ofrecer no solo medidas técnicas mejoradas, sino también programas educativos integrales para empoderar a los usuarios y mitigar los riesgos cibernéticos.

Se analizaron detalladamente las tecnologías de Amazon Web Services (AWS) y Microsoft Azure, evaluando su viabilidad para el desarrollo e implementación de la solución propuesta. La adopción de servicios como Amazon API Gateway, Lambda, DynamoDB, entre otros, ha sido crucial para establecer un entorno seguro y confiable para las transacciones en línea.

Además, se propuso un enfoque de respaldo mediante la nube de Microsoft Azure, como medida de contingencia ante posibles eventos inesperados que puedan afectar el servicio de AWS. Esta estrategia ofrece una garantía adicional, asegurando la continuidad de la generación de códigos CVC dinámicos incluso en situaciones de fallos en la infraestructura principal. La seguridad cibernética debe ser adaptable y flexible para hacer frente a posibles eventos imprevistos. La capacidad de cambiar entre proveedores de servicios en la nube asegura la continuidad del negocio y fortalece la defensa contra incidentes de seguridad.

Este documento representa un paso significativo hacia la creación de un entorno digital más seguro y confiable para las transacciones en línea. La combinación de medidas técnicas avanzadas, educación del usuario y un enfoque proactivo en la prevención de riesgos ha sentado las bases para una mayor protección de datos financieros, fortaleciendo la confianza de los usuarios y las entidades financieras en el ámbito de las transacciones electrónicas.

Se puede destacar la importancia de adoptar un enfoque integral para abordar los desafíos de seguridad en las transacciones en línea. Se resalta la necesidad de combinar medidas técnicas avanzadas con programas educativos para usuarios y entidades financieras, reconociendo que la seguridad cibernética es un esfuerzo colaborativo que requiere la participación de todos los actores involucrados. La educación de los usuarios y la cooperación entre entidades son esenciales para mitigar riesgos y crear un entorno seguro para las transacciones en línea.

En resumen, es esencial priorizar la seguridad y la confianza del cliente en el entorno digital, y esta prioridad debe reflejarse en la implementación de medidas técnicas avanzadas, programas educativos para usuarios y la adopción de estrategias de contingencia. Solo mediante un enfoque integral y colaborativo se puede crear un ecosistema de transacciones en línea más seguro y confiable para todas las partes involucradas.

REFERENCIAS

[1] E. M. Chimbo Encalada, «Desarrollo de una aplicación web progresiva para la gestión de reserva y pedidos del restaurante “EL FOGÓN DE COZ” implementando SSR,» 14 12 2022.

[2] E. P. L. Masabanda, «Sistema Web progresivo de comercio electrónico con pasarela de pagos online,» *Universidad Adventista de Bolivia. Cochabamba, Bolivia,* 10 01 2024.

[3] H. R. L. y. J. D. O. Patiño, «Estudio de Prefactibilidad para la Creación de Móvil Bank: Pasarela de Pagos 1 Digitales/corresponsal bancario en el Oriente Antioqueño,» *Estudio de Prefactibilidad para la Creación de Móvil Bank: Pasarela de Pagos 1 Digitales/corresponsal bancario en el Oriente Antioqueño,* 2022.

[4] N. B. PERICO, «Alerta por aumento de ciberataques en Colombia: hay 4 intentos de 'phishing' por minuto,» 20 11 2023.

[5] El Heraldo, «Siguen delinquiendo bajo la modalidad de smishing: ¿de qué se trata?,» 17 01 2024.

[6] D. A. L. B. y. J. T. Romero, «A mí también me pasó,» *El tiempo,* 04 09 2023.

[7] Pulso, «Sofisticada forma de robo de tarjetas de crédito de Bancolombia y compras en Falabella,» 04 07 2023.

[8] J. F. L. BRAN, «Gobierno investiga impacto de ataque cibernético que afectó a páginas de entidades,» *Organización Ardila Lülle - oal.com.co,* 13 09 2023.

[9] @ Cámara Colombiana de Comercio Electrónico 2024, «Conozca los principales desafíos de seguridad digital que tiene Colombia para el 2024,» 18 03 2024.

[10] @ Cámara Colombiana de Comercio Electrónico 2024, «CONOZCA LOS PRINCIPALES DESAFÍOS DE SEGURIDAD DIGITAL QUE TIENE COLOMBIA PARA EL 2024,» *CONOZCA LOS PRINCIPALES DESAFÍOS DE SEGURIDAD DIGITAL QUE TIENE COLOMBIA PARA EL 2024,* 18 03 2024.

[11] EL HERALDO S.A. , «Siguen delinquiendo bajo la modalidad de smishing: ¿de qué se trata?,» *Siguen delinquiendo bajo la modalidad de smishing: ¿de qué se trata?,* 17 01 2024.

[12] Copyright 2023 - Colombia Fintech, Asociación Colombiana de Empresas de Tecnología e Innovación Financiera, «Tokenización: la clave detrás de un pago por internet,» *Tokenización: la clave detrás de un pago por internet,* 18 02 2024.

[13] SEMANA S.A., «Ojo con las transacciones virtuales: ataques de ciberseguridad crecieron un 400 %,» *SEMANA S.A.,* 13 10 2022.

[14] R. A. V. ALAS, «Villatoro, R. (2015). Seguridad en las transacciones en línea de comercio electrónico. (Tesis de maestría no publicada). Universidad Don Bosco, San Salvador, El Salvador, C.A.,» *TRABAJO DE GRADUACIÓN SEGURIDAD EN LAS TRANSACCIONES EN LÍNEA DE COMERCIO ELECTRÓNICO,* pp. 3-20, 2015.

[15] C. d. E. M. L. A. R. d. B. Centrales, «CENTRO DE ESTUDIOS MONETARIOS LATINOAMERICANOS,» *Boletín , Volumen LV Número 1, enero-marzo 2009,* nº ISSN 0186-7229. , pp. 30-40, 2009.

[16] Cámara Colombiana de Comercio Electrónico, «Cámara Colombiana de Comercio Electrónico: INFORME DEL COMERCIO ELECTRÓNICO EN 2022 Y PERSPECTIVAS 2023,» 13 2 2023. [En línea]. Available: https://www.ccce.org.co/gestion_gremial/informe-del-comercio-electronico-en-2022-y-perspectivas-2023/ . [Último acceso: 18 8 2023].

[17] D. A. G.-A. C. A. E. G. L. C. A. A. M. S. E. G. John Alexander Arias Torres, «Blockchain aplicada en la innovación de proceso para la integración de servicios de tecnología financiera.,» Revista Virtual Universidad Católica del Norte, (69), 135-156, Bogotá, Medellín, Colombia, 2023.

[18] P. A. P. M. y. D. K. V. Silva, «Fundación Universitaria del Área Andina.,» 24 4 2023. [En línea]. Available: https://digitk.areandina.edu.co/handle/areandina/5027. [Último acceso: 17 8 2023].

[19] D. A. S. PEÑA, «Repositorio Institucional UNAD.,» 21 06 2023. [En línea]. Available: https://repository.unad.edu.co/handle/10596/56866. [Último acceso: 16 08 2023].

[20] L. D. H. CARDONA, «Repositorio Institucional UNAD,» 21 04 2023. [En línea]. Available: https://repository.unad.edu.co/handle/10596/55056. [Último acceso: 16 09 2023].

[21] N. S. Reyes, «La tecnología Blockchain y su potencial para revolucionar la gestión de datos y la seguridad de las transacciones,» 22 06 2023. [En línea]. Available: https://fipcaec.com/index.php/fipcaec/article/view/844. [Último acceso: 9 10 2023].

[22] A. A. G. GRIMALDOS, «Análisis de las normativas y estrategias de seguridad digital vigentes en la política nacional y su eficacia en el tratamiento de ciberdelitos en el sector de e-commerce durante COVID -19,» 19 09 2021. [En línea]. Available: https://repository.unad.edu.co/handle/10596/57182. [Último acceso: 08 10 2023].

[23] L. M. C. C. y. L. C. C. Rozo, «E-commerce: derechos y responsabilidades del consumidor en la adquisición,» 13 06 2023. [En línea]. Available: https://hdl.handle.net/10901/25389. [Último acceso: 9 10 2023].

[24] J. P. A. Torres Beltrán, «Implementación de las Fintech en Colombia Universidad Santo Tomás.,» 13 09 2022. [En línea]. Available: https://repository.usta.edu.co/handle/11634/47155. [Último acceso: 8 10 2023].

[25] M. K. H. Ramírez Soto, «Repositorio Institucional Universidad Norbert Wiener - Implementación de una pasarela de pagos en línea para el canal digital Tictuk en la empresa Delosi S.A.,» 22 04 2023. [En línea]. Available: https://repositorio.uwiener.edu.pe/handle/20.500.13053/8796. [Último acceso: 08 10 2023].

[26] A. V. LOAIZA, «El número de plataformas llegó a 97 firmas operando en 2018,» El número de pasarelas de pago en línea en Colombia ha crecido 53,9% LR - La Republica, 16 02 2019. [En línea]. Available: https://www.larepublica.co/internet-economy/el-numero-de-pasarelas-de-pago-en-linea-en-colombia-ha-crecido-53-9-2828821.

[27] C. d. C. Electrónico, «Datos clave para empresas que buscan robustecer los esquemas de seguridad en las transacciones en línea,» Nota de VTEX empresa afiliada a la CCCE, 11 4 2023. [En línea]. Available: https://www.ccce.org.co/noticias/datos-clave-para-

empresas-que-buscan-robustecer-los-esquemas-de-seguridad-en-las-transacciones-en-linea/.

[28] M. Garzón, «El reto de la banca en América Latina: que sus clientes usen más los canales digitales,» BBVA NOTICIAS, 2023. [En línea]. Available: https://www.bbva.com/es/el-reto-de-la-banca-en-america-latina-que-sus-clientes-usen-mas-los-canales-digitales/https://www.bbva.com/es/el-reto-de-la-banca-en-america-latina-que-sus-clientes-usen-mas-los-canales-digitales/.

[29] G. Cubides Toro, «Monitoreo transaccional de negocio Universidad Santo Tomás.,» 01 07 2023. [En línea]. Available: https://repository.usta.edu.co/handle/11634/51079. [Último acceso: 8 10 2023].

[30] E. M. S. V. C. T. I. Diana Roció Pérez Perilla, «Análisis de la percepción del cliente en la seguridad implementada a los servicios de la banca digital en Colombia: una revisión sistemática,» 07 05 2023. [En línea]. Available: https://digitk.areandina.edu.co/handle/areandina/5104. [Último acceso: 9 10 2023].

[31] Openbank, «Códigos de tarjetas: CSC, CVV, CVC, CVV2..., esas siglas que las protegen,» Open News Blog Openbank, 18 11 2019. [En línea]. Available: https://www.openbank.es/open-news/cvv-cvc-csc-codigo-seguridad-tarjeta/. [Último acceso: 8 10 2023].

[32] Teresa Andrés Blanco - BBVA Creative, «¿Qué es el CVV dinámico de una tarjeta? BBVA,» BBVA, 27 10 2020. [En línea]. Available: https://www.bbva.com/es/es/que-es-el-cvv-dinamico-de-una-tarjeta/. [Último acceso: 07 10 2023].

[33] Paula Calle Buencuerpo - Selectra, «Selectra, CVV o CVC de la tarjeta: tipos y cómo usarlo,» Selectra, 22 03 2023. [En línea]. Available: https://selectra.es/finanzas/tarjetas/cvv-o-cvc. [Último acceso: 07 10 2023].

[34] Teresa Andrés Blanco - BBVA, «BBVA Creative ¿Qué es el CVV dinámico de una tarjeta?,» BBVA Creative, 27 10 2020. [En línea]. Available: https://www.bbva.com/es/es/que-es-el-cvv-dinamico-de-una-tarjeta/. [Último acceso: 8 10 2023].

[35] «Mordor Intelligence,» 2023. [En línea]. Available: https://www.mordorintelligence.com/es/industry-reports/it-services-market. [Último acceso: 28 09 2023].

[36] «learn.microsoft.com,» 03 04 2023. [En línea]. Available: https://learn.microsoft.com/es-es/compliance/regulatory/offering-pci-dss. [Último acceso: 29 09 2023].

[37] S. A. EASTMAN, «La república,» Casi 30 millones de colombianos harán sus pagos en línea al cierre del año, 25 09 2023. [En línea]. Available: https://www.larepublica.co/especiales/revolucion-5-0/casi-30-millones-de-colombianos-haran-sus-pagos-en-linea-en-2023-3713312.

[38] S. V. C. &. A. V. A. L. y. C. Javier Vazquez, «Las 5 principales tendencias que guiarán las empresas en 2023,» https://www.visa.com.co © Copyright 1996 - 2023. , 2023. [En línea]. Available: https://www.visa.com.co/asociandose-con-nosotros/informacion-para-socios/blog/las-5-principales-tendencias-guiaran-empresas-2023.html.

[39] «El pais,» 7 04 2023. [En línea]. Available: https://www.elpais.com.co/economia/el-sector-de-software-y-servicios-ti-un-nuevo-pilar-del-mercado-laboral-en-colombia.html. [Último acceso: 28 09 28].

[40] A. A. G. GRIMALDOS, «ANÁLISIS DE LAS NORMATIVAS Y ESTRATEGIAS DE SEGURIDAD,» 2023. [En línea]. Available: https://repository.unad.edu.co/handle/10596/57182. [Último acceso: 9 10 2023].

[41] D. Betancourt, «Las Mejores pasarelas de pago para los comercios electrónicos B2B en Colombia,» © 2023 Sana Commerce , [En línea]. Available: https://www.sana-commerce.com/es/blog-es/mejores-pasarelas-de-pago-colombia/.

[42] FTC, «https://www.ftc.gov/,» 23 02 2023. [En línea]. Available: https://www.ftc.gov/news-events/news/press-releases/2023/02/new-ftc-data-show-consumers-reported-losing-nearly-88-billion-scams-2022.

[43] R. leyer, «https://www.usnews.com/,» 12 09 2023. [En línea]. Available: https://www.usnews.com/360-reviews/privacy/identity-theft-protection/identity-theft-fraud-

survey#:~:text=Identity%20Theft%20Losses&text=According%20to%20the%20FTC%2C%20online,private%20estimates%20are%20much%20higher..

[44] «https://www.juniperresearch.com/,» 12 10 2022. [En línea]. Available: https://www.juniperresearch.com/press/ecommerce-losses-online-payment-fraud-48bn.

[45] L. O. Barrios, «la nota economica,» Infobae, 22 06 2023. [En línea]. Available: https://www.infobae.com/colombia/2023/06/22/bogota-es-la-ciudad-de-colombia-donde-mas-ciberdelitos-se-cometen-cual-es-la-razon/. [Último acceso: 2023 10 3].

[46] Amazon, «Amazon API Gateway Cree, conserve y proteja las API a cualquier escala,» Amazon API Gateway, [En línea]. Available: https://aws.amazon.com/es/api-gateway/.

[47] Amazon, «AWS Lambda Ejecute código sin tener que pensar en los servidores o los clústeres.,» Amazon, [En línea]. Available: https://aws.amazon.com/es/lambda/?nc2=type_a.

[48] Amazon, «Amazon DynamoDB Servicio de base de datos NoSQL rápido y flexible para el rendimiento de milisegundos de un solo dígito a cualquier escala,» Amazon, [En línea]. Available: https://aws.amazon.com/es/dynamodb/?nc2=type_a.

[49] Amazon, «Amazon Relational Database Service Configure, opere y escale una base de datos relacional en la nube con tan solo unos clics.,» Amazon Relational Database Service, [En línea]. Available: https://aws.amazon.com/es/rds/?nc2=type_a.

[50] Amazon, «Amazon Simple Notification Service Servicio de publicación-suscripción totalmente administrado para mensajería A2A y A2P,» Amazon Simple Notification Service, [En línea]. Available: https://aws.amazon.com/es/sns/.

[51] Amazon, «Amazon CloudWatch Observe y monitoree los recursos y las aplicaciones en AWS, en las instalaciones y en otras nubes,» Amazon , [En línea]. Available: https://aws.amazon.com/es/cloudwatch/?nc2=type_a.

[52] © Microsoft 2023, «Microsoft Azure,» Microsoft Azure, 2023. [En línea]. Available: https://azure.microsoft.com/es-es/products/notification-hubs/.

[53] © Microsoft 2023 , «Microsoft Azure,» Microsoft Azure , 2023. [En línea]. Available: https://azure.microsoft.com/es-es/products/functions/.

[54] ©. M. 2023, «Microsoft Azure,» Microsoft Azure , 2023. [En línea]. Available: https://azure.microsoft.com/es-es/products/api-management/.

[55] © Microsoft 2023, «Microsoft Azure,» Microsoft Azure , 2023. [En línea]. Available: https://azure.microsoft.com/es-es/products/cosmos-db/.

[56] © Microsoft 2023, «Microsoft Azure,» Microsoft Azure , 2023. [En línea]. Available: https://azure.microsoft.com/es-es/products/azure-sql/database/.

[57] © Microsoft 2023, «Microsoft Azure,» Microsoft Azure , 2023. [En línea]. Available: https://azure.microsoft.com/es-es/products/monitor/.

[58] Statista Research Department, «Evolución anual del valor de las pérdidas por fraude de tarjetas de pago en Estados Unidos desde 2012 hasta 2018, según el tipo de fraude».

[59] © 2024 Stripe, Inc., «Estadísticas que predicen el futuro del fraude en línea y de e-commerce,» *Estadísticas que predicen el futuro del fraude en línea y de e-commerce,* 08 06 2023.

[60] © 2024 Stripe, Inc., «Estadísticas que predicen el futuro del fraude en línea y de e-commerce,» *Estadísticas que predicen el futuro del fraude en línea y de e-commerce,* 8 6 2023.

[61] © 2023, Amazon Web Services, Inc. o sus filiales. Todos los derechos reservados., «¿Qué es una interfaz de programación de aplicaciones (API)?,» © 2023, Amazon Web Services, Inc. o sus filiales. Todos los derechos reservados., [En línea]. Available: https://aws.amazon.com/es/what-is/api. [Último acceso: 28 05 2024].

[62] ©2024 Gartner, Inc. and/or its affiliates. All rights reserved., [En línea]. Available: Infraestructura Cloud https://www.gartner.com/en.

[63] ©2024 Gartner, Inc. and/or its affiliates. All rights reserved., «Digital Transformation: How to Scope and Execute Strategy,» *Digital Transformation: How to Scope and Execute Strategy.*

[64] F. publica, «funcionpublica.gov.co,» [En línea]. Available: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981.

[65] s. financiera, «Superfinanciera,» [En línea]. Available: https://www.superfinanciera.gov.co/publicaciones/10083443/normativanormativa-generalcircular-basica-juridica-ce-10083443/.

[66] pcisecurity, «pcisecurity,» [En línea]. Available: https://www.pcisecuritystandards.org/.

[67] ISO, «iso.org,» [En línea]. Available: https://www.iso.org/obp/ui/es/#iso:std:iso-iec:27001:ed-3:v1:en.

[68] M. G. S. y. M. J. M. Figueroa, «Introducción a las Fintech : alcance de su concepto y marco legal en Colombia Repositorio Institucional Universidad EAFIT,» 2023. [En línea]. Available: http://hdl.handle.net/10784/32627. [Último acceso: 09 10 2023].

[69] A. V. LOAIZA, «El número de pasarelas de pago en línea en Colombia ha crecido 53,9%,» *El número de plataformas llegó a 97 firmas operando en 2018,* 16 02 2019.