UNIVERSIDAD ESTATAL DE BOLÍVAR

FACULTAD DE CIENCIAS ADMINISTRATIVAS, GESTIÓN EMPRESARIAL E INFORMÁTICA

CARRERA DE SOFTWARE

TRABAJO DE INTEGRACIÓN CURRICULAR
PREVIO A LA OBTENCIÓN DEL TÍTULO DE
INGENIEROS EN SOFTWARE

FORMA: PROYECTO DE INVESTIGACIÓN

TEMA:

ESTUDIO DE LAS SEGURIDADES DE LAS TRANSACCIONES EN LÍNEA EN EL ECUADOR, AÑO 2022

AUTORES:

AYME PAREDES DARWIN ARIEL
SANDA CHIMBO RONALD EDUARDO

DIRECTOR:

ING. DARWIN CARRIÓN

GUARANDA – ECUADOR

2023

TEMA DEL PROYECTO DE INVESTIGACIÓN

ESTUDIO DE LAS SEGURIDADES DE LAS TRANSACCIONES EN LÍNEA EN EL ECUADOR, AÑO 2022

AGRADECIMIENTO

Agradezco a Dios por cada mañana darme las fuerzas para seguir adelante con mi carrera, por darme sabiduría para tomar buenas decisiones en el transcurso de mi vida universitaria, así mismo a mis padres por el amor desinteresado que han tenido conmigo, por el apoyo económico, sus valores y principios que los he llevado desde siempre y para siempre. A todos mis seres queridos por su ayuda y por confiar en mí. A mis profesores que con su comprensión supieron enseñarme la teoría para poderla aplicar en la práctica. Y especialmente a mi tutor Darwin Carrión quién supo servirme de guía para elaborar mi trabajo de titulación, por toda la paciencia brindada a lo largo de toda la tutoría del trabajo.

Ayme Paredes Darwin Ariel

A mi Dios todopoderoso que me brinda vida, salud, sabiduría y me continúa conduciendo por senderos de rectitud. A mi familia por apoyarme en todo momento ya que son la motivación que me impulsa a ser mejor cada día y a alcanzar los objetivos propuestos. Al Ing. Darwin Carrión, mi tutor en este trabajo de investigación, por su guía y entrega durante el desarrollo de este proceso. Finalmente, mi agradecimiento total a la Universidad Estatal de Bolívar en especial al personal y distinguidas autoridades de la Facultad de Ciencias Administrativas Gestión Empresarial e informática. Y a todos quienes de alguna u otra manera hicieron posible este logro.

Ronald Eduardo Sanda Chimbo

DEDICATORIA

A mi Dios en todo instante, su compañía y misericordia me han permitido llegar a este anhelado momento. Con él todo y sin él nada. Al pilar de mi vida que es mi familia, a mis padres Marco Ayme y Mirian Paredes, que a pesar de lo duro que fue para ellos el proporcionarme la educación siempre mantuvieron la meta de que cumpla mis sueños, que me enseñan que las metas se forjan con esfuerzo, dedicación, pero sobre todo con pasión, a mi hermana Mirelia y sobrina Natalia. Los amo con mi alma. A mis amigos y compañeros que a lo largo de todo este tiempo han estado conmigo. Y a mis docentes de la Carrera de Software por compartir sus experiencias y enseñanzas durante el tiempo compartido.

Ayme Paredes Darwin Ariel

Le dedico a Dios, porque sin su ayuda no hubiese podido terminar mi carrera. A mis padres Diego Sanda y Carmen Chimbo, a mis hermanas Mercedes y Sofía y a toda mi familia, por el apoyo incondicional que me han dado para poder estudiar fuera de mi ciudad natal, Y a todos aquellos que de alguna u otra manera hicieron parte de este proceso académico.

Ronald Eduardo Sanda Chimbo

CERTIFICADO DE VALIDACIÓN

UEB
UNIVERSIDAD ESTATAL DE BOLIVAR

FACULTAD DE CIENCIAS ADMINISTRATIVAS, GESTIÓN EMPRESARIAL E INFORMÁTICA

CERTIFICADO DE VALIDACIÓN

Ing. Darwin Carrión, Ing. Maricela Espín y Fis. Rafael Medina, en su orden Director y Pares Académicos del Trabajo de Integración Curricular "ESTUDIO DE LAS SEGURIDADES DE LAS TRANSACCIONES EN LÍNEA EN EL ECUADOR, AÑO 2022" desarrollado por los señores Ayme Paredes Darwin Ariel y Sanda Chimbo Ronald Eduardo.

CERTIFICAN

Que, luego de revisado el Trabajo de Integración Curricular en su totalidad, cumple con las exigencias académicas de la carrera SOFTWARE, por lo tanto, autorizamos su presentación y defensa.

Guaranda, 17 de noviembre del 2022

Ing. Darwin Carrión
Director

Ing. Maricela Espín
Par Académico

Fis. Rafael Medina
Par Académico

Dirección: Av. Ernesto Che Guevara y Gabriel Secaira
Guaranda-Ecuador
Teléfono: (593) 3220 6059
www.ueb.edu.ec

DERECHOS DE AUTORIA NOTARIZADA

DERECHOS DE AUTOR

Nosotros, **Ayme Paredes Darwin Ariel y Sanda Chimbo Ronald Eduardo** portadores de las cédulas de identidad **N° 0202677001** y **2101141873** respectivamente**,** en calidad de autores y titulares de los derechos morales y patrimoniales del Trabajo de Titulación: **ESTUDIO DE LAS SEGURIDADES DE LAS TRANSACCIONES EN LÍNEA EN EL ECUADOR, AÑO 2022,** modalidad Trabajo de Integración Curricular, de conformidad con el Art. 114 del CÓDIGO ORGÁNICO DE LA ECONOMÍA SOCIAL DE LOS CONOCIMIENTOS, CREATIVIDAD E INNOVACIÓN, concedemos a favor de la Universidad Estatal de Bolívar, una licencia gratuita, intransferible y no exclusiva para el uso no comercial de la obra, con fines estrictamente académicos. Conservamos a mi/nuestro favor todos los derechos de autor sobre la obra, establecidos en la normativa citada.

Así mismo, autorizamos a la Universidad Estatal de Bolívar para que realice la digitalización y publicación de este trabajo de titulación el Repositorio Digital, de conformidad a lo dispuesto en el Art. 144 de la Ley Orgánica de Educación Superior.

los autores declaran que la obra objeto de la presente autorización es original en su forma de expresión y no infringe el derecho de autor de terceros, asumiendo la responsabilidad por cualquier reclamación que pudiera presentarse por esta causa y liberando a la Universidad de toda responsabilidad.

Firmado electrónicamente por:
DARWIN ARIEL
AYME PAREDES

Darwin Ariel Ayme Paredes
CI. 0202677001

Firmado electrónicamente por:
RONALD EDUARDO
SANDA CHIMBO

Ronald Eduardo Sanda Chimbo
CI. 2101141873

ÍNDICE DE CONTENIDO

INDICE DE TABLAS

INDICE DE FIGURAS

INTRODUCCIÓN

Este estudio tiene como objetivo examinar la seguridad de las transacciones en línea en el comercio electrónico que actualmente es uno de los sectores de remesas más grandes del mundo, y todo indica que esta situación no solo persistirá, sino que crecerá exponencialmente en las próximas décadas. Según el informe Electronic Readiness realizado por Visa, demuestra que el crecimiento del comercio electrónico en América Latina convierte a la región en una de las regiones más atractivas del mundo para el crecimiento del comercio electrónico.

En el Ecuador los cambios sistémicos e inesperados derivados del Covid-19 impulsaron de manera abrupta a los emprendimientos ecuatorianos a deslastrarse del modelo tradicional del negocio. En este sentido, se vieron forzados a incorporar las tecnologías de innovación y comunicación dando como resultado el desarrollo del comercio electrónico, cuya característica principal es la facilidad que hay para comprar productos y/o servicios de forma segura. Ante el desarrollo del comercio electrónico, han aparecido nuevas entidades denominadas Fintech en la que se destaca la figura de pasarelas de pago, son proveedores de servicios financieros que tienen como beneficio su disponibilidad, accesibilidad y seguridad, avaladas por el Banco Central del Ecuador que constatan que cumplen con las funcionalidades de pasarelas de pago y estas son: Alignetsa S.A, Cardtech Ecuatoriana S.A, Ecuapayphone C.A, Kushki S.A, PagoPlux S.A, Paymentez (Nuvei), PlaceToPay.

Para analizar esta problemática es necesario mencionar sus factores causantes. Algunas de ellas son: la desconfianza existente en el comercio electrónico y se encuentra relacionado con los problemas de seguridad como: la privacidad, que trata de evitar que la información sea accedida por personas no autorizadas, la validación de la identificación, que identifica a la persona con la que se intercambia información, el no repudio, que asegura la validez de la firma existente en un documento electrónico y el control de integridad que asegura que la información transmitida a través de una red sea de forma segura. Para evitar estos problemas se han desarrollado diferentes herramientas, mecanismos y protocolos de pago seguro que garantizan la seguridad de las transacciones en línea y en donde se suma la importancia de estudiar las seguridades de las transacciones en línea en el Ecuador,

que diversos negocios de comercio electrónico han aplicado para garantizar la efectividad de sus transacciones.

Por lo expuesto se realizó una investigación de carácter descriptivo con un enfoque cualitativo, metodología de suma importancia al momento de indagar por los sitios oficiales de las pasarelas de pago en donde se recopilo información de las certificaciones como también de los protocolos de seguridad con los que se trabaja.

El trabajo de investigación se encuentra estructurado en cuatro capítulos. En el capítulo I, se revisa el tema de las transacciones en línea donde se planteó el siguiente interrogante ¿El desconocimiento de las seguridades existentes en las transacciones en línea impide el aumento del comercio electrónico? Además, se hace una reseña de las principales fuentes de información a fin de conocer su historia como también el estado actual del comercio electrónico.

En el capítulo II, se encuentran plasmadas las distintas amenazas que se presentan al momento de realizar una transacción en línea como también los mecanismo y protocolos de seguridad que se encuentran presentes en las pasarelas de pagos, para garantizar la seguridad de la información las cuales se verán reflejadas gracias a las certificaciones, mencionar que a lo largo de este capítulo presentamos los conceptos necesarios para entender los protocolos de pago seguro, con el objetivo de despejar las posibles incógnitas respecto a la seguridad en las transacciones.

En el capítulo III, se definió y aplicó el método de investigación más adecuado para cumplir con el objetivo de este trabajo de investigación. Primero, se presentó la teoría de las pasarelas de pago del Ecuador. Posteriormente se realizó las fichas de observación en donde se detalla que certificaciones, Protocolos y mecanismos de seguridad se encuentran incorporados y se concluye haciendo el análisis de los resultados obtenidos a través de este método.

En el capítulo IV, se encuentra establecido los resultados y discusiones en la que se encuentra a manera de detalle, un cuadro comparativo de las pasarelas de pago autorizadas por el Banco Central del Ecuador, donde se estableció el nivel de seguridad según los certificados y protocolos que han implementado.

Acrónimos y abreviaturas

ABREVIATURA	SIGNIFICADO
ASAP	Administradoras de los Sistemas Auxiliares de Pago
ATM	Cajero automático o Automated Teller Machine
AML	Lucha contra blanqueo de capitales
AVS	El Servicio de Verificación de Dirección
API	Interfaz de Programación de Aplicaciones
TIC´s	Tecnologías de la Información y las Comunicaciones
PCI DSS	Estándar de seguridad de datos de la industria de tarjetas de pago
CAST	Evaluación de Cumplimiento y Verificación de Seguridad
CECE	Cámara Ecuatoriana de Comercio Electrónico
CLV	Valor del tiempo de vida del cliente
CRM	Gestión de la relación con el cliente
CVV	Código Valor de Validación o Verificación
CNP	Card Not Present o tarjeta no presente.
UEES	Universidad de Especialidades Espíritu Santo
DEI	La Diversidad, la Equidad y la Inclusión
D-PAS	Aplicación de pago
DOI	Doble suscripción
DNS	Domain Name System o Sistema de nombres de dominio
EDI	Intercambio de los datos electrónicos
ERP	Sistema de planificación de recursos empresariales
EMV	Europay MasterCard VISA
GDPR	Reglamento General de Protección de Datos
IT	Tecnología de la Información
KYC	Know Your Customer (Conoce a tu Cliente)
SET	Transacción Electrónica Segura
TCP	Protocolo de Control de Transmisión
TLS	Seguridad de la capa de transporte
TTP	Trusted Third Party o tercero de confianza

TPV	Terminal-Punto de Venta
TELNET	Telecommunication Network
SAQ	Cuestionario de autoevaluación
SEM	Search Engine Marketing o Marketing de motores de búsqueda
SEO	Search Engine Optimization u optimización para motores de búsqueda
SIG	Sistema integrado de gestión
SGSI	Sistema de gestión de seguridad de la información
SSL	Capa de sockets seguros
SMTP	Protocolo simple de transferencia de correo
S/MIME	Extensiones seguras/multipropósito de correo de Internet
UNCTAD	Conferencia de las Naciones Unidas sobre Comercio y Desarrollo
OCDE	Organización para la Cooperación y el Desarrollo Económicos
OTP	Password o contraseña de un único uso o One-Time Password
PIN	Número de identificación personal
P2PE	Point to Point Encrypted o Encriptado Punto a Punto
RAM	Memoria de Acceso Aleatorio
ROI	Retorno de Inversión (Return On Investment)
ICPEN	La Red y el Cumplimiento de Protección del Consumidor Internacional
ICV	Valor de verificación de integridad
IP	Dirección del Protocolo de Internet
WWW	World Wide Web o red informática mundial
FTP	Protocolo de Transferencia de Ficheros
URL	Localizador de Recursos Uniforme
HTTPS	Protocolo de transferencia de hipertexto

RESUMEN

En la actualidad de la Globalización es muy difundido el uso del Internet, por tanto, es importante tener en cuenta que las transacciones que se realicen se hagan de manera segura, y sobre todo de acuerdo a la legislación vigente en el Ecuador. Las transacciones en línea del comercio electrónico en el Ecuador han tenido un gran impacto en el mercado; los consumidores realizan transacciones de compra y venta de productos y/o servicios de forma electrónica cada vez con mayor frecuencia, no obstante, es importante identificar, cuál es el inconveniente que ocurre al momento de verificar si este tipo de comercio es totalmente seguro. Se presentan diversos factores que ponen a las transacciones en línea como vulnerables en aspectos de seguridad de los datos. Para resolver estos problemas se han desarrollado e implementado tecnologías como las pasarelas de pago que proporcionan seguridad al momento de realizar transacciones en línea. El objetivo principal de esta investigación es estudiar la seguridad en las transacciones en línea, debido a los continuos delitos que existen al respecto. Se utilizó el método de investigación descriptiva, en donde se hizo la descripción de todos los elementos que hacen parte del proceso en las transacciones electrónicas a través del Internet. Los resultados evidencian que las seguridades que poseen las pasarelas de pago están conformadas por diversos protocolos y mecanismos de seguridad, por lo tanto, se concluye que el uso de esos servicios garantiza la eficiencia, eficacia y sobre todo proporciona la seguridad a los usuarios.

PALABRAS CLAVES: Comercio electrónico, Transacciones en línea, Protocolos de seguridad, Pasarelas de pago.

ABSTRACT

In today's globalization, the use of the Internet is very widespread, therefore, it is important to take into account that the transactions are made safely, and especially according to the current legislation in Ecuador. Online transactions of electronic commerce in Ecuador have had a great impact on the market; consumers make transactions of purchase and sale of products and / or services electronically with increasing frequency, however, it is important to identify, what is the drawback that occurs at the time of verifying whether this type of trade is totally safe. There are several factors that make online transactions vulnerable in terms of data security. To solve these problems, technologies such as payment gateways have been developed and implemented to provide security when making online transactions. The main objective of this research is to study the security of online transactions, due to the continuous crimes that exist in this regard. The descriptive research method was used, where the description of all the elements that are part of the process in electronic transactions through the Internet was made. The results show that the security features of payment gateways are made up of various protocols and security mechanisms, therefore, it is concluded that the use of these services guarantees efficiency, effectiveness and above all provides security to users.

KEY WORDS: Electronic commerce, Online transactions, Security protocols, Payment gateways.

CAPÍTULO I

FORMULACIÓN GENERAL DEL PROYECTO

1.1. Descripción del Problema

El comercio electrónico sin duda alguna, ha permitido realizar transacciones en línea de compra y venta de bienes y servicios de forma rápida y eficaz a través de las plataformas digitales; en el Ecuador este modelo de negocio ha obtenido un gran crecimiento en los últimos tiempos, debido a que se ha ido transformando en una de las mejores alternativas más notorias en las actividades comerciales, el uso de las transacciones en línea como medio de pago. Según la Cámara Ecuatoriana de Comercio Electrónico (2021) la Superintendencia de Bancos del Ecuador contempla todas las transacciones en línea que se registran en el país; al comparar el índice del uso de las transacciones en línea que se realizó en el 2019 respecto al 2020 y el período de enero a abril del 2021, Ecuador creció más de 19 millones en términos de transacciones en línea. También se registró un crecimiento, entre el 2020 hasta abril del 2021, de 4.1 millones de transacciones hechas con tarjetas de crédito a través de e-Commerce y 552 millones de ventas que se realizaron a través de tarjetas de crédito. La información mostrada refleja en términos generales que las transacciones en línea se están haciendo presente cada vez más y más en el quehacer diario de los ecuatorianos, la cual, en un futuro no muy lejano, este modelo de comercio va ser sin duda la más empleada debido a sus múltiples facilidades y ventajas que proporciona en el comercio.

Sin embargo, cabe destacar que pese a los diversos beneficios que proporciona las transacciones en línea, ha sido complicado obtener la aceptación generalizada de la ciudadanía, debido a diversos factores que tienen que ver con la seguridad, la confianza en el uso de las transacciones en línea y sobre todo al desconocimiento por parte de los usuarios; que las transacciones en línea contemplan un completo esquema de seguridad que proporciona tanto el banco como también la entidad intermediaria que son las pasarelas de pagos, las cuales avalan a través de certificaciones y protocolos de seguridad que las transacciones sean efectuadas de manera correcta y sin contratiempos en su proceso.

Las vulnerabilidades que sufren las transacciones en línea generan en los usuarios una desconfianza hacia la confidencialidad de los datos, ya que comprometen información confidencial como pueden ser, el número de la tarjeta de crédito, el número de la cuenta bancaria, los datos personales entre otros. La información sin duda es lo más valioso que poseen y es por tal motivo que buscan siempre mantenerlas protegidas, evitando así exponerlas.

El problema que se presenta en el Ecuador según el Ministerio de Telecomunicaciones y de la Sociedad de la Información (2020) en su informe ejecutivo indica que, la privacidad o protección de datos es la principal preocupación de los usuarios. El riesgo de robo o suplantación de identidad y especialmente el fraude financiero ha generado una conciencia elevada respecto a las amenazas que pueden existir al momento de realizar transacciones en línea, impidiendo al comercio electrónico alcanzar su potencial. Esto se resume en la negativa por parte de la ciudadanía para realizar transacciones en línea.

1.2. **Formulación del Problema**

¿El desconocimiento de las seguridades existentes en las transacciones en línea impide el aumento del comercio electrónico?

1.3. **Preguntas de Investigación**

¿Cuáles son los tipos de amenazas en la seguridad de las transacciones en línea?

¿Cuáles son los protocolos de seguridad que se aplican para una transacción en línea segura?

¿Cuáles son las empresas que brindan el servicio de pasarela de pagos autorizadas por el Banco Central del Ecuador?

¿Qué mecanismos o estrategias de seguridades han implementado las empresas que brindan el servicio de pasarela de pagos?

1.4. **Justificación**

Las transacciones en línea han agilizado las formas de pago a través de las distintas plataformas digitales, una de las muchas facilidades que proporciona las transacciones en línea, es que se puede realizar desde cualquier lugar con acceso a internet, hoy en día el internet se encuentra desplegado por la mayor parte del

territorio ecuatoriano, lo que brinda comodidad al usuario realizar la transacción desde el hogar, la oficina o donde se encuentre.

Las cifras del crecimiento que han tenido las transacciones en línea se ven evidenciadas en todo el mundo y Ecuador no es la excepción. Según Ponce (2021) en su informe indica que entre 2019 y 2020 se ha multiplicado la cantidad de usuarios que realizan transacciones en línea, del 2% al 10%, demostrando el potencial de mercado en Ecuador, el comercio electrónico se incrementó en un 23,9% durante 2021.

El comercio electrónico en el mercado de compras en línea, beneficia a las dos partes de la transacción; tanto a los negocios por la reducción de costos de almacenamiento y exhibición, como a los consumidores, teniendo acceso a una mayor gama de productos en menor tiempo, sin la necesidad de movilizarse y con la seguridad que proporciona la transacciones en línea hoy en día. Barros (2010) afirmó que "la seguridad en el comercio electrónico y específicamente en las transacciones en línea es un aspecto de suma importancia, puesto que brinda confianza tanto a proveedores como a compradores que hacen del comercio electrónico su forma habitual de negocio".

Esta investigación contribuirá con información valiosa acerca de las seguridades en las transacciones en línea, permitiendo tener una idea profunda de los requerimientos como también de los mecanismos y protocolos de seguridad que se deben implementar para disponer de un comercio electrónico seguro. Además, ayudará a los ecuatorianos a desarrollarse dentro del mundo del e-Commerce & e-Business permitiendo crear fidelidad; para lograr que la población aproveche exitosamente los beneficios que brinda esta tecnología, se debe garantizar la autenticidad, confidencialidad, integridad y el no repudio en la red.

Esta investigación se encuentra enfocada a la línea de investigación, Gestión De Tecnologías de la Información y Comunicación y a la Sublínea de investigación, valoración integral de las TIC´s para la toma de decisiones.

1.5. **Objetivos:**

1.5.1 Objetivo General

Estudiar las seguridades de las transacciones en línea, que diversos negocios de comercio electrónico han aplicado para garantizar la efectividad de sus transacciones.

1.5.2 Objetivos Específicos

- Estudiar los diferentes tipos de amenazas que se presentan en las transacciones en línea.
- Identificar los protocolos de seguridad que se aplican para una transacción en línea segura.
- Analizar las diferentes empresas que brindan el servicio de pasarela de pagos en el Ecuador.
- Investigar si las empresas de pasarela de pagos cumplen con la certificación PCI DSS (Payment Card Industry Data Security Standard).

1.6. **Idea a Defender**

El estudio y difusión de las seguridades existentes para las transacciones en línea contribuirá a mejorar la confianza de los usuarios en utilizar el comercio electrónico en el Ecuador.

CAPÍTULO II

MARCO TEÓRICO

2.1. Antecedentes

Con el desarrollo progresivo del internet se ha visto nuevos modelos de negocios relacionados con el comercio electrónico; actividades como la compra y venta de productos y servicios a través de las tiendas virtuales, haciendo uso de las transacciones en línea como método de pago, que aporta beneficios en aspectos como la reducción de costos, tiempo de adquisición y sobre todo en lo fácil que se hace al cliente poder adquirir algún producto o servicio y pagar de manera rápida y eficaz.

El Ministerio de Telecomunicaciones y de la Sociedad de la Información (2020) señala que el aumento en el uso de internet como también el descubrimiento de las nuevas tecnologías y en particular, el desarrollo de las Tecnologías de la Información y Comunicación (TIC), han facilitado y sobre todo han proporcionado nuevas e innovadoras formas de comercializar productos y servicios. Dando como resultado el comercio electrónico con múltiples beneficios para las empresas, los consumidores y la sociedad.

2.1.1. Comercio Electrónico en el Mundo

Según Orús (2022) en los últimos años, y especialmente a partir de la pandemia de COVID-19, que apareció en el año 2019, la cual azotó a nivel mundial, el comercio electrónico se ha convertido en una parte indispensable del mercado global. Y es que, durante años, la manera de como las diferentes empresas comerciales estaban ofreciendo sus productos cambiaron drásticamente, al modelo de comercializar sus productos de manera limitada y con muchas restricciones en la movilidad humana; las empresas optaron a nuevas formas de mover la economía, es ahí donde el comercio electrónico se hiso presente con más relevancia y el Internet fue el único medio a través del que muchas empresas pudieron seguir generando ingresos. No en vano, cerca del 90% de la población mundial admitió haber comprado en Internet en 2020, razón por la que nos sorprende que los ingresos procedentes de las ventas

online se situaran en alrededor de 4,2 billones de dólares estadounidenses en dicho año. Esta cifra fue aún mayor en 2021 pese a la apertura de los comercios, lo que no hace sino dejar constancia de que este cambio en los hábitos de compra es con casi toda seguridad permanente.

Ahora a nivel mundial, podemos encontrar una variedad de portales y tiendas virtuales que están plenamente dedicadas al comercio electrónico de todo tipo de productos y servicios. La cual indica que este modelo de comercializar tanto productos como servicios ha dado un giro en su totalidad dejando atrás pero no obsoletas a las compras tradicionales, demostrándonos nuevamente que el comercio electrónico tiene un gran auge y con múltiples beneficios que proporciona a la sociedad. La producción creada por la sociedad está lazada altamente por las actividades que generan la vida cotidiana, habiendo una alta demanda de productos y servicios a ser adquiridos con una facilidad para las personas las cuales han promovido a la revolución tecnológica. La expansión que ha generado las TIC a lo largo de su trayectoria ha creado la posibilidad que nuevas industrias puedan surgir y ser capaces de fomentar una economía estandarizada para su desarrollo, sin embargo, al progresar de la mano con la tecnología esta ha perdido sus características vitales del modelo tradicional.

Según Jara (2020) las grandes empresas como Amazon, Alibaba y JD.com son quienes están encabezando la lista del e-Commerce ya que estas representan el 72% de las ventas por vía online en todo el mundo. Tienen proyecciones sumamente altas a largo plazo, deduciendo que para el 2025 el e-Commerce tomará el 10% del control de todo el gasto económico mundial generado por los usuarios como de organizaciones que hagan el uso de las mismas. Esta cifra es el doble de la actualidad por lo que sería un gran avance económico para estas empresas que buscan tener mayor accesibilidad en la economía de las naciones en el mundo. Agregando a esto, sistemas en la telecomunicación como el e-Commerce, la integración de la tienda física, la tecnología inteligente y opciones de venta directa al consumidor, sumarán nuevos compradores por vía online superando sus números actuales que corresponden al 21% entre los consumidores actuales de sus productos.

2.1.2. Comercio Electrónico en América Latina

El comercio electrónico en América latina aumento a partir de la pandemia COVID-19, resultado de las restricciones en la movilidad humana como también de los productos, la mayoría de los gobiernos de América latina han implementado medidas para fomentar y hacer uso del comercio electrónico como alternativa al comercio tradicional durante la pandemia. Según Jara (2020) un reporte de la Comisión Económica para América Latina (2018) indica que la región representará el 6% dentro del comercio económico mundial y su desarrollo internacional que lo caracteriza como nueva integración dentro de la economía. La institución estima que el 38% del e-Commerce estará explícitamente de la mano con este cambio y a los efectos de sus actividades.

La realidad en la que se basa América Latina sobre el e-Commerce ha sido identificada por el portal Expreso, en el reporte de Linio (2017) donde la lista de los países con mayor utilización de este servicio está liderada por Chile con un gasto promedio de US$314, seguido por México con US$139, Perú tiene US$125, Argentina US$95.8, Brasil US$94 y Colombia US$80.6.

Por ende, el comercio electrónico viene a constituirse una actividad en auge. Que se ve evidenciada tanto a nivel mundial como a nivel continental e internacional, en los últimos años se ha visto un gran desarrollo tecnólogo la cual es notable en América Latina. Ahora bien, existe factores que impiden su despegue y consolidación. Uno de estos factores es la desconfianza que impera en la Red por parte del consumidor o usuario. Estos factores impiden el desplegué total y el uso de las transacciones en línea en la sociedad por ende existen personas que la utilizan cotidianamente como también a las personas que le es difícil utilizar y no por interactuar con tecnologías nuevas y tal vez les cueste entender y utilizar, si no por la desconfianza que genera mover su dinero de forma digital y realizar acciones financieras desde los dispositivos tecnológicos (López & Redchuk, 2016).

Según estudios realizados sobre la percepción de compras en internet, en la actualidad aproximadamente el 71% de los compradores piensa que comprar en internet es seguro y tiene muchas ventajas. Es por esto también que se puede notar un aumento en las personas que optan por realizar compras y pagar con transacciones en línea, las tendencias han cambiado, en un principio la gente

desconfiaba del internet y sus servicios ya que sentían que les estaban de cierta manera engañando. A pesar de que esta tendencia ha ido cambiando, hoy en día el mayor reto para el comercio electrónico es generar confianza en los usuarios. Concretamente en América Latina el desarrollo y el crecimiento del comercio electrónico tiene que ver con los diferentes medios de pagos que están disponibles en las páginas web de las empresas (Merino, 2015).

2.1.3. Situación Actual del Comercio Electrónico en Ecuador

La situación del comercio electrónico en el Ecuador, Según el Ministerio de Telecomunicaciones y de la Sociedad de la Información (2020) en su informe ejecutivo muestra que la emergencia sanitaria provocada por la pandemia del COVID-19 está impulsando el comercio electrónico y la transformación digital a nivel mundial. A medida que la pandemia golpea todos los rincones del mundo, ha obligado a los consumidores a cambiar de las compras tradicionales a las compras en línea, haciendo uso como método de pago las transacciones en línea. De esta forma, el comercio electrónico se convierte en un ámbito privilegiado, aunque continúa un proceso constante de crecimiento y maduración debido a la aparición y cambio de necesidades tanto de proveedores como de consumidores.

Un estudio de la Cámara Ecuatoriana de Comercio Electrónico (CECE) y la Universidad de Especialidades Espíritu Santo (UEES) encontró que el 40% de las empresas creará herramientas de comercio electrónico para ofrecer aún más sus servicios. En Ecuador, las compras digitales se han multiplicado por lo menos 15 veces desde el inicio del distanciamiento social, abriendo el comercio electrónico y logrando que el 34% de los usuarios de plataformas digitales estén constantemente en una plataforma digital. Para aquellos que han usado la plataforma pocas veces o nunca la usan ahora lo están empezando a utilizar.

Según eCommerce Institute (2022) el e-Commerce Day Ecuador Blended [Professional] Experience se llevó a cabo del 1 al 3 de junio de forma Blended. Esta es una iniciativa regional del e-Commerce Institute organizada a nivel local por la Cámara Ecuatoriana de Comercio Electrónico (CECE).

Más de 3000 personas pudieron asistir y participar en una plataforma de eventos de 3 días dedicada a la especialización del sector Retail, con los principales expertos de la industria digital. La conferencia, las sesiones plenarias y los eventos temáticos

en vivo fueron vistos más de 7000 veces, y más de 1200 personas asistieron al e-Commerce Day presencial. Las últimas tendencias y casos de éxito se revelan en sesiones en vivo y seminarios web. Durante la conferencia se analizó el estado de los negocios digitales dentro del país.

Danny Barbery Montoya, Decano de la Facultad de Comunicación de la UEES, habló sobre el estado actual, desafíos y tendencias del comercio electrónico en el Ecuador y la región. A medida que crecemos de 2021 a 2022, se espera que nuestras ventas crezcan aproximadamente un 180 % en millones de dólares para fin de año. La cantidad de personas que compran en dispositivos móviles aumentó un 10% desde el 58% en 2020. Las redes sociales y WhatsApp son los canales preferidos para las compras offline.

Durante el 2022 los usuarios eligen utilizar tarjeta de crédito para pagar, generando un aumento del 43% con respecto a 2020. Se anunciaron los ganadores del Premio de los e-Commerce Awards Ecuador 2022. Crear estos premios es distinguir a las empresas en la industria digital de negocios y al negocio de Internet. A partir del presente año, el e-Commerce Institute reconocerá a las iniciativas digitales orientadas a promover la Sostenibilidad y la Diversidad, Inclusión y Equidad (DEI), para ello, sumó dos nuevas categorías a los e-Commerce Awards: eWomen y e-Commerce Award Triple Impacto. Presentamos a continuación a los ganadores de cada categoría:

Líderes del e-Commerce en la Industria Turística: Oro Verde, Líderes del e-Commerce en Retail: Créditos Económicos, Entretenimientos y Medios en e-Commerce: Supercines, Mejor proveedor de servicios de IT y soluciones para eCommerce: Servientrega, Servicios Financieros y Banca Online: Paymentez, Indumentaria y moda en e-Commerce: Tennis, Mejor Agencia de e-Commerce: Known Online, Mejor Pyme en e-Commerce: Marpesia, Mejor iniciativa Mobile en e-Commerce: Tipti.

En primer lugar, se llevó a cabo el "Análisis de seguridad informática en transacciones electrónicas" Sabogal (2021) en su examen presentada para tener derecho al título de experto en seguridad informática, considerando la capacidad de planificar el comercio electrónico en el futuro, que comprende el comercio y los negocios, no solo se centra en grandes empresas y/o corporaciones internacionales,

ya que hay muchas empresas medianas y pequeñas que proporcionan sus productos y servicios a través de plataformas electrónicas. En donde contar con el uso adecuado de las tecnologías van a facilitar a todas las entidades a emprenderse en el uso de las transacciones en línea como método de pago.

Tello & Pineda (2017) en la tesis "Análisis del comercio electrónico en el Ecuador" para la Universidad Internacional del Ecuador encontraron que el proyecto de investigación pretende ampliar la perspectiva del lector sobre las transacciones de comercio digital, brindando datos interesantes sobre la evolución del comercio electrónico los alcances de esta nueva forma de hacer negocios. Por lo tanto, es necesario identificar los factores que inciden en el desarrollo del comercio electrónico en el Ecuador, así como los factores que inciden en el desempeño de las transacciones de los consumidores a través de Internet. Además, se analizarán las ventajas y desventajas que trae el comercio electrónico a los consumidores y empresas.

Por otro lado, el gobierno de la república del Ecuador mediante el Ministerio de Telecomunicaciones y de la Sociedad de la Información (2020) presenta un informe ejecutivo "Estrategia Nacional de Comercio Electrónico" en donde se argumenta que el creciente uso de internet, la aparición de nuevas tecnologías y en particular, el desarrollo de las Tecnologías de la Información y Comunicación (TIC) han posibilitado la generación de innovadoras maneras de comercializar productos y servicios, permitiendo a las empresas superar barreras geográficas y de tiempo. El comercio electrónico es la consecuencia natural de este panorama, que brinda múltiples beneficios para las empresas, los consumidores, la sociedad y en general para la economía de un país, dado que permite reducir costos y tiempos de operaciones, fomenta la producción con valor agregado y genera fuentes de empleo. Ante esta situación, se requieren habilidades digitales para utilizar el comercio electrónico, pero Ecuador enfrenta una brecha digital con respecto a los países regionales y globales que representa una desventaja competitiva en este nuevo escenario de negocios, diagnosticada como significativa.

De igual manera Salas (2010) en su trabajo titulado "Seguridad de las Transacciones de Comercio Electrónico", presentado a la Corporación

Universitaria de la Costa en la Facultad de Derecho de Barranquilla en el año 2010, afirma que el uso del uso de Internet es muy común en esta era de globalización, por lo que es importante tener en cuenta que las transacciones se realicen de manera segura y sobre todo en cumplimiento de la legislación vigente.

El objetivo principal de esta investigación es establecer la seguridad de las transacciones electrónicas debido al delito que se desarrolla en el campo. Se utilizó un método de investigación descriptivo, en el cual se describen todos los factores que intervienen en el proceso de transacciones electrónicas por Internet. En resumen, se puede decir que es necesario exigir regulaciones acordes con los avances tecnológicos y los nuevos sistemas de delincuencia en Internet.

Villatoro (2015) presentó el tema “Seguridad de las transacciones en línea en el comercio electrónico” a la Universidad Don Bosco en febrero de 2015, donde señaló que es importante tratar de determinar dónde surge el mayor inconveniente al momento de la verificación, en caso de que el uso de este tipo de transacción se vuelva completamente inseguro o menos confiable durante el manejo.

Analizamos esto examinando la vulnerabilidad a la que se expone una empresa cuando se violan sus sistemas de seguridad, junto con la información confidencial almacenada en sus servidores, como: números de tarjetas de crédito, números de cuentas bancarias, datos personales, etc. Para este inevitable problema, es necesario lidiar con los protocolos de seguridad, ya que gracias a ellos hacemos un gran trabajo protegiendo la información de los usuarios con encriptación de datos, métodos de autenticación, firewalls, etc.

2.2. Científico

2.2.1. Seguridades en las Transacciones Electrónicas

Según Saúl (2015) en el artículo "Comercio electrónico: la importancia de la seguridad en las transacciones electrónicas, Amenazas y Soluciones de implementación" argumenta que la mayoría de los consumidores tienen una comprensión clara de qué esperar cuando se hace clic en "Aceptar" en Internet. La transacción, que es el proceso que se realiza cuando conecta su tarjeta a un cajero automático y paga en línea, técnicamente hablando, sigue estos procesos. Lo que

sucede es que se simplifica la gestión del software, incluyendo protocolos para garantizar la seguridad de estas transacciones. Cuando se trata de protocolos de seguridad, muchas personas se encargan de asegurarlos, pero siempre existe la posibilidad de que los atacantes puedan descifrarlos, por lo que empresas especializadas se encargan de desarrollar nuevos sistemas y diferentes para crear mejores versiones o nuevos protocolos más complejos.

El protocolo SET utiliza cifrado para garantizar la máxima privacidad durante la transmisión y validación de firmas digitales, lo cual es imprescindible para los comerciantes digitales autorizados por un banco o institución financiera. El protocolo permite agregar información personal entre un cliente y un comerciante y entre un cliente y una institución financiera en una misma transacción, proceso conocido como doble firma y tiene una estructura criptográfica. Otros protocolos de seguridad que solemos usar o aplicar son TLS Transport Layer Security (TLS, Transport Layer Security) y su antecesor, Secure Sockets Layer (SSL, Secure Connection Layer). Ya lo sabíamos cuando configuramos nuestras cuentas de correo electrónico en nuestros dispositivos móviles.

2.2.2. Seguridad de los Pagos en Línea

Según la Organización de Naciones Unidas (2017) en su conferencia sobre la "Conferencia de las Naciones Unidas sobre Comercio y Desarrollo" señaló que los pagos en línea y móviles se realizan a través de Internet, usando computadoras o dispositivos móviles activos, usando cuentas personales. abierta antes de la transacción. El uso de dispositivos móviles por parte de los consumidores para pagar transacciones de comercio electrónico está aumentando con el desarrollo de la tecnología.

Como se establece en el Manual de Protección al Consumidor de la Conferencia de las Naciones Unidas sobre Comercio y Desarrollo (UNCTAD), se espera que los pagos móviles representen el 3% de los pagos de comercio electrónico en 2017. pagos a consumidores en algunos países en desarrollo, especialmente aquellos donde la mayoría de la población no tiene acceso a servicios financieros.

Sin embargo, los sistemas de pago en línea y móviles pueden ser problemáticos para los consumidores, exponiéndolos a una variedad de riesgos de seguridad. Los terceros no autorizados pueden acceder a los datos de los consumidores sin su

conocimiento y consentimiento. Los problemas observados en los países en desarrollo y abordados en las respuestas al cuestionario de la UNCTAD incluyen retrasos en la recepción de pagos por parte de los comerciantes; pago irreversible; demora de confirmación; y casos de bloqueo de pagos entre un banco, pasarela de pago o empresa receptora de pagos sin que el consumidor sepa dónde se detuvo el proceso. Algunos de estos problemas pueden estar relacionados con un Internet subdesarrollada. En Alemania, por ejemplo, al 13 % de los consumidores se les cobra injustificadamente por servicios de terceros.

La recomendación de la Organización para la Cooperación y el Desarrollo Económicos (OCDE) insta a los gobiernos y otras partes interesadas a garantizar un nivel mínimo de protección al consumidor en los pagos de comercio electrónico, independientemente del mecanismo adoptado. Las directrices de la OCDE sobre la protección del consumidor en el contexto de los pagos móviles y en línea tienen como objetivo promover la protección del consumidor y otras prácticas industriales en el sector de los pagos móviles y en línea. al tiempo que reconoce los beneficios que las innovaciones en el sistema de pago aportan a los consumidores.

Según la Red y el Cumplimiento de Protección del Consumidor Internacional (ICPEN), en la aplicación general de la protección del consumidor en el pago móvil, alienta a las partes a participar en pagos móviles para aplicar cuatro reglas para obtener un alto nivel de protección en todo el tipo de Pago: el mecanismo de seguridad debe ampliarse; Los consumidores no deben ser responsables de las transacciones ilegales; Se establecerán restricciones a las responsabilidades del consumidor en caso de transacciones ilegales, correspondientes al nivel de negligencia del consumidor; Y los consumidores recibirán información clara y relevante sobre cada compra, condiciones de comercio de contratos y mecanismos de compensación existentes. ICPEN alienta a las partes a prestar atención a los consumidores que pueden ser más sensibles que su edad, inexperiencia o falta de habilidades informáticas.

2.2.3. Protección de los Datos y la Vida Privada

Según la Organización de Naciones Unidas (2017) en la conferencia titulada "Conferencia de las Naciones Unidas sobre Comercio y Desarrollo" señaló que las compras en línea pueden ser más riesgosas para los consumidores que otros

métodos no electrónicos. A medida que aumenta el uso de tarjetas de crédito y débito para pagar las compras en línea, también aumenta la frecuencia con la que los comerciantes recopilan y venden la información personal de los consumidores. Los datos personales son valiosos para las empresas en línea, ya que enriquecen su conocimiento del mercado y les permiten crear perfiles de consumidores individuales. Los problemas que surgen con respecto a la protección de la privacidad y los datos incluyen, con la excepción, la falta de comprensión de cómo se utilizan los datos recopilados en Internet, determinando la responsabilidad en caso de una violación de la seguridad de los datos.

Las Recomendaciones de la OCDE tienen como objetivo proteger la privacidad de los consumidores al garantizar que sus prácticas en relación con la recopilación y el uso de la información del consumidor sean legales, transparentes y justas, permitan a los consumidores participar y tomar decisiones, al tiempo que brindan garantías de privacidad y seguridad. Alentando a las empresas a proteger su privacidad. La sección 49 establece que las empresas deben "manejar las amenazas a la seguridad digital e implementar medidas de seguridad para minimizar los impactos negativos en la participación del consumidor en el comercio electrónico".

2.2.4. Elementos de seguridad de la información del comercio electrónico

Según Villatoro (2015) la seguridad de la información se sustenta en los siguientes pilares, que ayudan a construir controles de seguridad robustos:

La Integridad se refiere a garantizar que los datos no serán manipulados por usuarios no autorizados. Es cierto que el comercio electrónico simplifica las transacciones, haciéndolas cada vez más eficientes, pero es necesario definir claramente el primer factor, porque sin él no puede haber honestidad en el procesamiento y habrá signos inesperados de falsificación de la información, lo que resulta en un bajo nivel de satisfacción al participar en este modelo atípico.

No repudio se da cuando garantizamos que los beneficiarios del comercio electrónico no puedan negar el intercambio ya finalizado, una vez hayan ejercido cualquier proceso en línea, sirve como prueba del origen, la autenticidad y la integridad de los datos. Asegura al remitente que el mensaje fue entregado y prueba

la identidad del remitente al destinatario. De esta forma nadie puede negar que un mensaje ha sido enviado, recibido o procesado.

La Autenticidad se refiere a la secuencia de pasos que realizamos para obtener la plena verificación de la verdadera identidad de una persona física o jurídica basada en el hecho de que los datos obtenidos del solicitante corresponden al cliente. Bienes o empresas sin encontrar un intermediario haciéndose pasar por ellos (suplantación de identidad).

La Confidencialidad en este momento es donde nos aseguramos de que la información transmitida a través de la red sea utilizada de forma segura por el usuario que solicita un pedido o por la empresa que recibe la solicitud de un cliente que ha utilizado sus servicios.

La Disponibilidad se refiere a la capacidad de un sitio de comercio electrónico para ser flexible, evitar interrupciones y funcionar correctamente las 24 horas del día. Independientemente de cuándo se necesita la solicitud para satisfacer sus necesidades.

2.3. Conceptual

2.3.1. Seguridad en las transacciones electrónicas

Según Jara (2020) en el comercio electrónico para que su desarrollo transcurra sin problemas se necesitan varios factores, factores como el control y la seguridad han dado paso a sistemas como la criptografía, destinados a codificar matemáticamente mensajes en un formato ilegible la cual conduce a la retención de datos oficiales generados por usuarios y organizaciones que afectan su desempeño. Actualmente, los estándares de seguridad y prevención requieren que los sistemas de pago cumplan adecuadamente con los requisitos establecidos para garantizar la seguridad del usuario, tales como: privacidad de datos, autenticación e integridad de datos.

Por lo tanto, las transacciones en línea tienen encriptación de fuente abierta y especificaciones de seguridad diseñadas para proteger las transacciones con tarjeta de crédito o débito en Internet. Las transacciones electrónicas no son un sistema de pago, sino un conjunto de protocolos y formatos seguros para garantizar el uso seguro de las transacciones de pago en línea.

2.3.2. Amenazas en las transacciones en línea

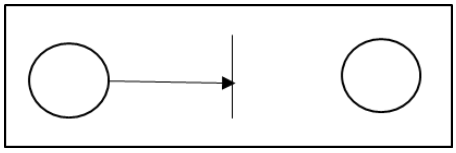
Según Molina (2007) las amenazas que se pueden encontrar en las transacciones en línea tienen el potencial de causar daño, pero no son una debilidad concreta, un ataque no es más que la implementación de una amenaza, mientras que la vulnerabilidad ocurre cuando el sistema es vulnerable a un ataque laboral. Por lo tanto, podemos decir que una amenaza es una intención específica de explotar las vulnerabilidades del sistema en otros términos generales es la posibilidad de una fisura de seguridad por la ocurrencia de situaciones, ocasiones, acciones o eventos que puedan amenazar la seguridad y causar un daño.

Dejando a un lado las amenazas en las transacciones en línea vamos hablar de los ataques que vienen a ser un ataque a la seguridad del sistema causado por una amenaza, es un acto razonable e intencional de eludir los servicios y violar la política de seguridad del sistema. Estos ataques a su vez se encuentran distribuidos de la siguiente manera.

Las interrupciones son recursos del sistema que están dañados, no disponibles o inutilizables. Es un ataque a la usabilidad. Por ejemplo, destruir un dispositivo de hardware, cortar las comunicaciones o apagar un sistema de administración de archivos.

Figura 1

Ataque de interrupción



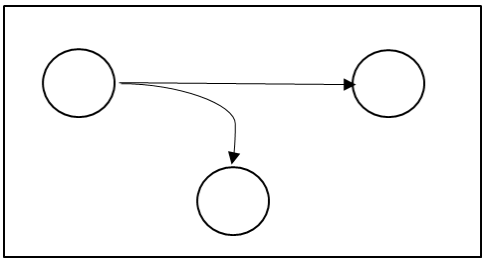
Nota: El gráfico representa a un ataque de interrupción, este es un ataque contra la usabilidad. Tomado de *Seguridades en Comercio Electrónico,* por Molina, 2007, Universidad del Azuay.

Así mismo una intercepción ocurre cuando una parte no autorizada tiene acceso a un recurso. Es un ataque a la privacidad. La entidad no autorizada puede ser una

persona, un programa o una computadora. Ejemplo: interceptar una línea para recibir datos que circulan por la red.

Figura 2

Ataque de Intercepción

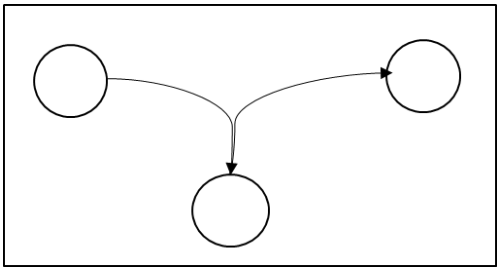


Nota: El gráfico representa a un ataque de Intercepción, este es un ataque contra la privacidad. Tomado de *Seguridades en Comercio Electrónico,* por Molina, 2007, Universidad del Azuay.

Otro ataque es la modificación, cuando una persona no autorizada no solo obtiene acceso a la autenticación, sino que también la rompe. Esto es un ataque a la integridad. Por ejemplo, cambiar un valor en un archivo de datos, cambiar un programa para que se comporte de diferente manera cambiando el flujo de proceso correspondiente a si mismo cambiar el contenido de los mensajes enviados a través de la red.

Figura 3

Ataque de Modificación

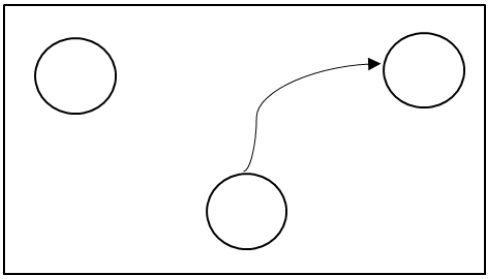


Nota: El gráfico representa a un ataque de Intercepción, este es un ataque contra la integridad. Tomado de *Seguridades en Comercio Electrónico,* por Molina, 2007, Universidad del Azuay.

La fabricación ocurre cuando una entidad no autorizada inserta objetos no autorizados en el sistema. Este es un ataque a la autenticidad, un ejemplo de tal ataque es inyectar mensajes ilegales en la red o agregar entradas a un archivo.

Figura 4

Ataque de Autenticidad



Nota: El gráfico representa a un ataque de Intercepción, este es un ataque contra la autenticidad. Tomado de *Seguridades en Comercio Electrónico,* por Molina, 2007, Universidad del Azuay.

Estos ataques también se pueden clasificar útilmente en ataques pasivos y ataques activos.

Los ataques pasivos es cuando el atacante no cambia la conexión, sino que la escucha o la manipula para enviar la información. Su primordial objetivo es la recopilación de datos y el análisis del tráfico, un método más sofisticado para extraer información de los mensajes. Estos ataques vienen a ser difíciles de detectar porque no dañan sus datos; Sin embargo, su éxito puede evitarse cifrando la información.

En cambio, los ataques activos implican y realizan algún tipo de modificación en el flujo de información transmitida y se encuentran divididas en cuatro categorías mencionadas a continuación:

Suplantación ocurre cuando el atacante se hace pasar por otra unidad. Por ejemplo, las cadenas de autenticación se pueden interceptar y recuperar, lo que permite a los usuarios obtener acceso a ciertos recursos privilegiados, dando como posible resultado el robo de contraseñas de cuentas.

Re actuación referente a la reproducción que ocurre cuando se graban y repiten uno o más mensajes legítimos para causar efectos no deseados, como realizar depósitos y enviarlos varias veces a una cuenta en particular.

Modificación del mensaje: parte de un mensaje válido ha sido alterada, o el mensaje ha sido retrasado o reordenado con efecto no autorizado.

Degradación del Servicio Falso: Inhabilitar o impedir el uso normal de la gestión de los recursos informáticos y de comunicación. Por ejemplo, un atacante podría eliminar todos los mensajes enviados a una entidad en particular, o una red podría verse comprometida al inundarse con mensajes ilegítimos. Estos ataques incluyen ataques de denegación de servicio, desactivación temporal de servidores de correo, WWW, FTP, etc.

Muchas de estas actividades maliciosas tienen como objetivo el fraude, el phishing y más. Las amenazas externas más comunes a la web son:

- Virus, gusanos y caballos de Troya.
- Spyware y adware.
- Ataques de día cero, también llamados “ataques de hora cero”.
- Ataques de piratas informáticos.
- Ataques por denegación de servicio.
- Interceptación y robo de datos.
- Robo de identidad.

Los ataques pueden venir desde un inocente correo electrónico hasta el insertar una memoria removible sin el previo cuidado de pasarlo por el antivirus.

Las vulnerabilidades en la web según Sabogal (2021) indica que este tipo de fraude se realiza mediante la explotación de una vulnerabilidad en el código del sitio web; Los estafadores pueden cambiar el precio de los bienes, siempre reduciendo significativamente su valor.

Legalmente, no se puede probar que esto fue intencional y que no fue un error, los costos casi siempre corren a cargo de la empresa sin ningún tipo de reclamación. Para mitigar este tipo de ataques, es importante que las empresas tengan un sitio

web que haya sido probado previamente y probado exhaustivamente para detectar vulnerabilidades por un equipo de expertos y certificados en esta área.

2.3.3. Amenazas de seguridad

De acuerdo con la Superintendencia de Bancos del Ecuador, los delincuentes tienen diferentes formas de engañar a los usuarios para obtener claves, algunas de estas formas son:

2.3.3.1. Phishing.

Según Parrilla (2015) señala que el término phishing en relación con las palabras "pescar" es un intento de obtener información confidencial como contraseñas, datos de cuentas bancarias, tarjetas, etc. de una manera inusual haciéndose pasar por un síndico vía correo electrónico o Messenger usando URLs similares.

Las principales características de los correos electrónicos que intentan obtener información personal son:

- Contenido de aspecto realista: el correo electrónico parece haber sido enviado por la empresa que dice ser. Logotipos, enlaces de contacto, estilos de sitios, avisos de derechos de autor y más. copiado. Incluso pueden contener un enlace real a un sitio web legítimo.
- Solicita información confidencial sin preguntar. Ningún negocio serio debería enviar spam sin que se le solicite hacer clic en un enlace que solicita información confidencial.
- Saludos genéricos: Estos correos electrónicos se envían de forma masiva y aleatoria a un gran número de personas, por lo que el saludo siempre es muy general.
- Enlaces disfrazados: los enlaces contenidos en el correo electrónico están presentados para que parezcan auténticos.
- Imágenes con enlaces: el correo completo es una imagen que se puede pulsar para acceder al enlace fraudulento.
- Urgencia en la respuesta: la redacción del correo da sentido de urgencia al usuario en la respuesta o envío de datos.

Ante alguna sospecha de que un correo electrónico recibido pueda ser fraudulento, se recomienda verificar lo siguiente:

- Dominio de correo electrónico: la verificación más simple que se puede hacer es asegurarse de que el dominio de correo electrónico coincida teóricamente con la empresa que envía el correo electrónico.
- Cuenta equivocada: si el usuario tiene varias cuentas de correo electrónico, debe verificar que la que proporcionó a su compañía es la misma en la que está recibiendo el correo electrónico.
- Archivos adjuntos: los archivos enviados por empresas legítimas suelen estar en formato PDF. Es conveniente consultar archivos en cualquier formato de Microsoft Office o que pidan permiso para ejecutarlos.
- Seguridad SSL: si se accede a alguno de los enlaces que proporciona el e-mail, se debe verificar que la página web a la que se redirige está utilizando una dirección HTTPS.
- URL engañosa: antes de hacer clic en un enlace, debe pasar el cursor sobre el enlace para asegurarse de que pertenece a una empresa legítima.
- Formas en el correo: un e-mail con campos para suministrar directamente datos sensibles, es fraudulento.

2.3.3.2. Pharming.

Según Parrilla (2015) señala que esta estafa consiste en redirigir al cliente a una página que se parece a la página original de su banco, en la misma página que recopila la contraseña secreta cuando las ingresa, incluida la precedencia DNS (Domain Name Settlement System) para dirigir a los usuarios a un sitio de phishing. Un atacante logra esto alterando la traducción entre la URL (Localizador Uniforme de Recursos) de una página y su dirección IP.

El DNS es como una guía telefónica en Internet. Cada vez que ingresa una dirección de Internet, en realidad está llamando a una dirección IP. Dado que sería una tarea difícil recordar todas las direcciones IP que nos interesan, los servidores DNS hacen el trabajo por nosotros: enviamos el nombre del sitio a visitar, y automáticamente navegan en la lista de su directorio para obtener la dirección IP del sitio web que desea visitar.

Por lo general, los atacantes redirigen a sitios web falsos con código malicioso. Entonces, después de ingresar a un dominio específico que ha sido modificado, el navegador web accede al sitio web especificado por el atacante para ese dominio. Para ser redirigido a sitios web falsos, un atacante debe poder instalar una aplicación o programa malicioso (malware) en el sistema de la víctima. El código malicioso puede ingresar a su sistema de varias maneras, más comúnmente por correo electrónico, pero también puede descargarlo de Internet o usar dispositivos de almacenamiento masivo como USB.

La gran diferencia entre las estafas phishing y pharming es el nivel de actividad del usuario. En caso de phishing, el usuario debe acceder a la dirección que le envió el atacante, y en el caso de pharming, solo debe acceder al DNS modificado.

2.3.3.3. Smishing.

Según GcfGlobal (2022) el término hace referencia a un delito en el que los delincuentes utilizan mensajes de texto para engañar a las víctimas con concursos falsos o premios inexistentes en un sitio web que contiene un virus. Para evadir estos ataques debemos evitar dar datos por mensajes de texto y no creer en rifas o regalos ya que estas formas son las principales formas de enganchar a las personas a que logren acceder y otorgar información relevante,

2.3.3.4. Vishing.

Según GcfGlobal (2022) en este caso, el delincuente se comunica con la víctima a través de llamadas telefónicas en las que lo engañan para que revele su información personal con el fin de apropiarse de sus fondos. Cómo evitarlo: No haga transferencias o transacciones utilizando un número de teléfono diferente al de tu banco.

2.3.3.5. Key logger.

Según GcfGlobal (2022) usando software o hardware, los delincuentes registran discretamente todo lo que escribe en su teclado y lo guardan en otro lugar. Entonces, al realizar una transferencia a través de Internet, la víctima está revelando sus datos a los estafadores. Cómo evitar esto: actualice su computadora o dispositivo móvil

con un programa antivirus apropiado. No utilice dispositivos públicos para realizar transacciones.

2.3.3.6. Skimming.

Cuando una persona lleva su tarjeta de crédito a una tienda, los delincuentes la colocan a través de un dispositivo llamado skimmer que registra información de la banda magnética y luego la escribe en una tarjeta falsa.

Según Computerworld (2022) el robo de tarjetas mediante el skimming es un tipo de ataque en el que se introduce un dispositivo o mecanismo malicioso en el momento de una transacción legítima para recopilar los datos de la tarjeta. En el mundo físico, se coloca un dispositivo de desnatado en la ranura de una tarjeta de cajero automático para recopilar datos codificados. Suelen ir acompañados de una pequeña cámara o superposición en un panel PIN (Número de identificación personal) para registrar el código PIN introducido por el usuario. El cambio a tarjetas inteligentes que usan encriptación junto con otras funciones de autenticación y transacción tiene como objetivo contrarrestar estas tarjetas.

Los ataques de navegación web o digital se basan en principios similares, pero usan código malicioso para capturar datos de las tarjetas que son ingresados a través de los formularios de los usuarios. Este código malicioso ingresa a los sitios web de varias maneras: utilizando credenciales administrativas débiles o robadas, explotando vulnerabilidades en aplicaciones web que permiten a los atacantes cargar código no autorizado en un servidor web o pirateando servicios de terceros.

Los grupos skimming de navegación por Internet utilizan técnicas sofisticadas para que sea difícil de revelar sus códigos de registro de teclas. El código puede ser muy complejo y agregarse a archivos JavaScript existentes o almacenarse en otros recursos como CSS (hojas de estilo en cascada) o incluso incrustarse en imágenes.

2.3.3.7. Adware.

Kaspesrky (2022) señala que el adware es un programa diseñado para mostrar anuncios en su computadora, redirigir sus búsquedas a sitios web publicitarios y recopilar información comercial sobre usted (como los tipos de sitios web que visita) para mostrarle anuncios dirigidos. No confunda el software adware (que

recopila datos con su consentimiento) con los troyanos de software adware que recopilan datos sin su consentimiento. Si un anuncio no le dice que está recopilando datos, se considera dañino. Por ejemplo, el malware explota el comportamiento de espionaje del troyano.

2.3.3.8. Spyware.

Redesna (2022) menciona que el spyware es un software que recopila datos de una computadora y los transmite a una organización externa sin el conocimiento o consentimiento del propietario de la computadora. Estos programas están diseñados para monitorear la navegación web del usuario. El software no se propaga como los virus; Por lo general, se instala utilizando una vulnerabilidad.

El término "spyware" también se usa de manera más general para referirse a otros productos que realizan varias funciones, como mostrar anuncios no deseados (emergentes), recopilar información personal, redirigir solicitudes de página e instalar marcadores. Un programa típico de software espía se instala en el sistema de la víctima de tal manera que se inicia cada vez que se enciende la computadora (usando CPU y RAM, lo que reduce la estabilidad de la computadora) y se ejecuta todo el tiempo, monitoreando el uso de Internet y datos relacionados demás de mostrando consecutivamente anuncios publicitarios, Sin embargo, a diferencia de un virus, no intenta reproducirse en otras computadoras y por lo tanto se comporta como un parásito.

2.3.3.9. Tarjetas de crédito robadas.

Según Sabogal (2021) da a conocer que este tipo de fraude se da en todas las empresas electrónicas y el objetivo no es más que conseguir el acceso al producto antes de que la empresa detecte que la tarjeta ha sido robada. Es muy riesgoso para el comercio electrónico enviar productos digitales y entregarlos a los clientes de inmediato. La mejor manera de limitar este tipo de fraude, especialmente para las pequeñas y medianas empresas, es utilizar un TPV (Terminal-Punto de Venta) de un banco, porque de esta forma toda la responsabilidad recae en el banco. y esta organización es responsable de comprobar la tarjeta.

2.3.3.10. Devolución forzosa.

Sabogal (2021) dice que esto ocurre cuando el banco del usuario o cliente descuenta el pago recibido, generalmente después de aceptar una compra fraudulenta. Sin embargo, hay otros dos casos en los que la devolución es forzosa, comprenda:

A través de PayPal o proveedores similares: Cuando un estafador vincula una tarjeta robada a su cuenta de PayPal y realiza una compra sin la menor sospecha. PayPal puede tardar 6 meses en hacer el reverso.

Voluntario: Quizás el estafador está haciendo un uso perfecto de tu tarjeta o cuenta, entonces el cliente contacta al banco y alega que la compra se realizó sin su consentimiento o que es víctima de un robo de tarjeta.

2.3.4. Protocolos de seguridad en las transacciones en línea

Se conoce que Internet representa un canal de comunicación inseguro, debido a que un potencial atacante puede acceder fácilmente a la información que se distribuye en esta red en cualquier momento. Datos transmitidos entre dos nodos en Internet, ejemplificando entre su computadora y el servidor web desde el que intenta descargar la página se dividen en pequeños paquetes que son enviados por varios nodos remotos diferentes para llegar a su destino.

Dentro de cada paquete, puede leer, destruir e incluso modificar el contenido del paquete, permitiendo acceder a todo tipo de ataques a la seguridad y la integridad de los datos. El ejemplo más conocido y comprensible de esta situación es que la postal puede ser vista por carteros, vecinos o familiares, por lo que no nos basamos en absoluto en información sensible para evitarlo. En el caso de Internet, la forma más común de crear un análogo digital de esta capa es utilizar los protocolos SSL y SET.

2.3.4.1. Protocolo SSL (Secure Sockets Layer).

Según Molina (2007) SSL fue desarrollado e implementado por Netscape Communications Corporation en 1994 con el primer lanzamiento de Navigator. Sin embargo, solo después del lanzamiento de la tercera versión llamada SSL v3.0, se solucionaron los problemas y las limitaciones de seguridad del predecesor. En su

forma actual, proporciona cifrado de datos, autenticación de servidor, integridad de mensajes y opciones de autenticación de cliente para conexiones TCP/IP.

SSL v3.0 es tan funcional que es tan conocido ya que se usa ampliamente en Internet esto debido a que es compatible con todos los principales navegadores del mercado, por lo que no se requiere ninguna acción especial para activar este protocolo. Simplemente basta con hacer clic en el enlace o abra una página con una dirección que comience con https://. Y ya el resto se encarga el navegador. Por supuesto, debemos asegurarnos de que SSL esté habilitado en el navegador.

SSL se usa especialmente en la comunicación de hipertexto, pero también se puede usar en otros protocolos, porque SSL es la capa debajo de HTTP y, como sugiere el nombre, está en el nivel de socket, por lo que no solo está usando protección de hipertexto. Documentos, así como servicios como FTP, Protocolo simple de transferencia de correo (SMTP), redes de telecomunicaciones (TELNET), etc.

Actuando como una máquina de estado, siempre hay un estado de escritura activo y en espera durante la comunicación. Se utiliza un subprotocolo de negociación llamado Change Cipher Spec para cambiar de modo activo a pasivo, se pueden abrir múltiples sesiones SSL entre dos clientes y el servidor, aunque esto no es común, se pueden cambiar y mantener múltiples conexiones SSL en una sola sesión. Las conexiones se abren o cierran mediante un protocolo de Handshake.

Transacciones basadas en SSL

Según Buch & Jordán (2022) señalan que posiblemente debido a la dificultad de implementar SET, la mayoría de los sistemas comerciales ahora se basan en SSL en lugar de SET, lo que debilita la seguridad. Estos sistemas a menudo se denominan punto de venta virtual (TPV virtual).

La principal desventaja de los pagos SSL es la incapacidad de firmar digitalmente el pedido de una transacción en línea, lo que elimina la necesidad de que el comprador tenga un certificado digital. Finalmente, el problema de que los comerciantes tengan acceso a los números de tarjetas de crédito de los clientes se resuelve alojando un punto de venta virtual en una pasarela de pago (ubicada en una institución financiera) y requiriendo la autenticación del vendedor.

Para mitigar el riesgo asociado a la imposibilidad de realizar una autenticación fuerte del comprador (solo basta con tener un número de tarjeta con saldo para completar la transacción), la llamada tarjeta virtual, que se caracteriza por la presencia de un número saldo fijo, se agota y requiere de ser recargada posteriormente para poder seguir utilizándola.

Pagos SSL

La pasarela de pago SSL se activa cuando el comprador quiere pagar tras seleccionar los productos deseados.

1. El vendedor informa al portal que desea realizar el cargo en la tarjeta de crédito o débito del cliente. Para ello, envía el importe a cargar, un enlace al TPV virtual. Esto incluye la autenticación fuerte del vendedor en el punto de venta virtual (a través del canal SSL y el certificado generado por la puerta de enlace).
2. El comprador es redirigido a un punto de venta virtual que le proporciona la cantidad, los datos de la empresa y un enlace para comprar. La conexión entre el cliente y el TPV virtual es vía SSL, pero únicamente mediante autenticación del servidor, lo que asegura que el cliente envía los datos al servidor correcto.
3. El comprador introduce el número de tarjeta.
4. El TPV virtual obtiene de la pasarela de pagos el resultado de la transacción presentándose al cliente e informando al comerciante.
5. El TPV virtual redirecciona al comprador al comercio.
6. Finalmente, los comerciantes pueden administrar de forma remota un POS virtual con el reconocimiento adecuado. Las operaciones que se pueden realizar son operaciones "batch", operaciones de carga y consultas en general. Una operación adicional que permiten algunos TPV virtuales es la operación manual, que funciona como un TPV clásico.

2.3.4.2. Protocolo SET (Transacciones electrónicas seguras).

Según Molina (2007) SET es un protocolo estandarizado respaldado por la industria, diseñado para asegurar las compras con tarjeta en redes abiertas, incluido

Internet. El estándar SET fue desarrollado en 1995 por Visa y MasterCard en colaboración con otras empresas líderes como Microsoft, IBM, Netscape, RSA, VeriSign y otras. Tan pronto como se finalizó el protocolo SET 1.0, la infraestructura comenzó a surgir lo que respaldó su uso generalizado. Muchos proveedores de software han comenzado a crear productos para consumidores y minoristas que desean comprar de forma segura.

Servicios del Protocolo SET, uno de los más importantes es la autenticación, donde todas las partes involucradas en una transacción comercial que son los clientes, comerciantes y bancos, editores y compradores, pueden usar certificados para verificar la autenticidad de los demás. Esto permite que el comerciante verifique la identidad del titular de la tarjeta y que el comprador verifique la identidad del comerciante. De esta manera, puede evitar el fraude con tarjetas y las empresas en línea que se hacen pasar por sitios web de grandes empresas. Los bancos, a su vez, pueden usar esto para verificar la identidad del propietario y el vendedor.

Del mismo modo, tenemos la confidencialidad y políticas de datos y la privacidad, importantes en las que tratamos de proteger su información de pago para que no sea espiada. Esto significa que SET simplemente va descifrar el número de la tarjeta de crédito, por lo que ni siquiera el comerciante puede verlo para evitar el fraude. Si desea encriptar el resto de la información de su compra, como los artículos comprados, debe usar un protocolo de seguridad más bajo como SSL.

Por otro lado, la integridad asegura que toda la información intercambiada no se pueda cambiar accidental o maliciosamente mientras se navega por la red utilizando algoritmos de firma digital. En cuanto a la Gestión del pago SET gestiona tareas relacionadas con actividades comerciales de alta importancia como el registro de propietarios y vendedores, autorización y liquidación de pagos, cancelaciones, entre otras.

La verificación instantánea es uno de los servicios más importantes de SET, ya que proporciona a los vendedores una verificación instantánea de la identidad del comprador como también el saldo existente en su cuenta antes de realizar una compra. De esta manera, el vendedor puede cumplir con los pedidos sin el riesgo de que la transacción sea cancelada más adelante. Otra ventaja y así misma de igual

importancia sobre otros sistemas de seguridad es la adición de un estándar de certificado digital que conecta la identidad de los tarjetahabientes y comerciantes con las instituciones financieras y los sistemas de pago como Visa, MasterCard, etc.

Transacciones basadas en SET

Con la facilidad y colaboración de los principales proveedores de computadoras y software, Visa y MasterCard han desarrollado lo que se está convirtiendo en el principal protocolo de pago para el comercio electrónico minorista (es decir, la compra y venta entre comerciantes y usuarios finales). SET un protocolo que simula el pago electrónico de bienes y/o servicios con tarjeta de crédito mediante el uso de certificados y firmas digitales.

En el sistema SET se cuida hasta el más mínimo detalle, en lo que corresponde a la seguridad de las transacciones en línea utilizando las últimas tecnologías de autenticación y firma digital para proteger los datos en Internet. Todos los participantes de SET deben tener un certificado válido para participar en las transacciones de pago en línea lo que significa que tanto el propietario como al proveedor deben estar predefinidos y certificados para funcionar en el sistema.

Protocolo de Pago SET

El protocolo SET define los mensajes y las interacciones de las entidades SET como lo son los compradores, comerciantes y pasarelas de pago, para completar una transacción de pago en línea desde el momento en que el comprador acepta pagar hasta que se realiza el pago se debe seguir una secuencia de acciones las cuales son mencionadas a continuación.

1. Fase Inicial: la fase inicial corresponde a mensajes PINit que es en donde el comprador contacta al vendedor seguidamente el comprador declara la marca de la tarjeta utilizada para el pago y el comerciante responde con un mensaje firmado que contiene el certificado criptográfico de la pasarela de pago correspondiente.
2. Fase de Pago esta etapa corresponde al anuncio en el que el comprador acepta el pago luego de verificar la identidad y condición del vendedor. La

respuesta a este mensaje contiene información sobre cómo aceptar o rechazar la autorización de pago.

3. Fase de Autorización esta etapa corresponde a un mensaje de validación donde el comerciante pregunta a la pasarela de pago si el comprador puede realizar el pago especificado (con crédito o saldo, tarjeta no invalidada, etc.). La respuesta a este mensaje indica que el pago ha sido aceptado o rechazado. En este programa, se decidió reparar o recibir el pago dentro del mismo período de autorización.

También cabe recordar que SET implementa un sistema de doble firma donde el comprador en el mensaje de PReq incluye datos seguros para el comerciante y para la pasarela de pago, de manera que el vendedor solo ve los datos de compra (pedidos, forma de pago, cantidad, etc.), y la pasarela de pago solo ve los detalles del pago (número de tarjeta, método de pago, cantidad, etc.) que se enviarán en el mensaje AuthReq. De esta forma el comerciante jamás tendrá acceso al número de la tarjeta del comprador y la entidad financiera a través de la pasarela de pago nunca tendrá información detallada de la compra.

2.3.4.3. Protocolo TLS (Transport Layer Security).

Según Navarro et al. (2014) TLS es básicamente un protocolo de comunicación que establece una conexión segura y fiable entre un cliente y un servidor a través de un canal encriptado. Está desarrollado a partir de su predecesor SSL (Secure Sockets Layer) creado por Netscape1. El intercambio de información con TLS/SSL se realiza en un entorno seguro y libre de ataques la cual son ampliamente necesarios en el tránsito de información debido a:

Eavesdropping que viene a ser una de las formas más insidiosas de llevar a cabo ciberataques y su método de ejecución es la de robar datos escuchando a escondidas de manera ilegal en el tráfico de la red, una forma de espionaje conocida como Eavesdropping, debido a que el usuario ignora los ataques de spyware y exponen información confidencial, como lo es las contraseñas, números de cuentas bancarias, contenido de correo electrónico e incluso hábitos de navegación a los piratas informáticos. Los ciberdelincuentes pueden incluso interceptar llamadas telefónicas VoIP.

Como también el protocolo TLS en su esencia Evitar la falsificación de la identidad del remitente manteniendo la integridad de la información en una aplicación cliente-servidor. Además, posee la capacidad de intercambiar parámetros criptográficos sin necesidad de que ninguna de las dos conozca partes el código de la otra. Por último, mencionar que como es conocimiento de la mayoría los algoritmos criptográficos son costosos computacionalmente, por lo que el protocolo incluye un esquema de caché de sesiones para reducir el número de sesiones que deben inicializarse desde cero.

2.3.4.4. Protocolos de seguridad 3D Secure.

Según Parrilla (2015) la tecnología 3DSecure agrega un paso adicional de autenticación a los pagos en línea y está diseñada para prevenir el fraude de compras en línea, como el fraude CNP (Card No Present), además de otorgar seguridad y confianza a los clientes en sus transacciones en línea.

Para realizar pagos con tarjeta en línea, los compradores deben proporcionar los detalles de su tarjeta. Esta información se puede recuperar fácilmente de la tarjeta para su uso posterior sin presentar la tarjeta, lo que facilita la comisión de fraude

Se requiere información adicional para confirmar el pago al usar el servicio 3DSecure. Si alguien obtiene la información de la tarjeta de crédito/débito o incluso si se la roban, no podrá comprar en línea porque el estafador desconoce la información adicional otorgada por el protocolo y estará protegida. Para realizar pagos en 3DSecure, la tarjeta debe ser 3DSecure y la tienda en línea debe admitir el protocolo 3DSecure. Si alguna de las partes, la tarjeta o la tienda, no es compatible con la tecnología 3DSecure, su compra no estará protegida por el protocolo. Según la ley, al pagar con 3DSecure, el banco del consumidor es el responsable de la transacción, ya que es él quien confirma la identidad de la persona que realiza la compra. Esta responsabilidad pasa directamente al consumidor ya que solo él o ella necesita conocer la información confidencial para trabajar con 3DSecure.

El funcionamiento del protocolo 3DSecure para los pagos en línea conlleva a un proceso habitual la cual es ingresar los datos de su tarjeta. Luego, la tienda en línea

envía la transacción al sitio web del emisor de la tarjeta, donde se requiere información adicional para autenticar al titular de la tarjeta. Después de ingresar esta información, la transacción será devuelta a la tienda en línea para la confirmación del pago. De esta forma, el banco asegura a la tienda online que quien paga es realmente el titular de la tarjeta.

Adicional cabe resaltar que las marcas que han desarrollado previamente este protocolo y que son muy utilizadas en todos los portales de Internet son Visa con el programa Verified by Visa y Mastercard con el programa MasterCard SecureCode.

2.3.4.5. MasterCard SecureCode.

Según Parrilla (2015) el protocolo MasterCard SecureCode es un servicio de seguridad que protege contra el uso no autorizado de su Tarjeta MasterCard cuando compra en línea en los distintos comercios que lo integran. Asimismo, reduce el número de disputas que surgen al permitir autenticar al titular de la tarjeta en el momento de la compra, minimizando así los costes asociados a los contracargos.

No es necesario comprar una nueva tarjeta o descargar ninguna aplicación para usar este programa, por lo que no hay cargos. Al suscribirse a este servicio, tendrá más confianza en que MasterCard SecureCode tomará un paso adicional de autenticación para proteger su tarjeta. Para registrar su tarjeta con MasterCard SecureCode y obtener sus propios códigos de autenticación, puede hacerlo solicitándolos a la entidad emisor de su tarjeta antes de realizar la compra o al mismo tiempo que realiza la compra y pago en línea.

2.3.4.6. protocolo Verified by Visa (VbV).

Según Parrilla (2015) el protocolo Verified by Visa es un programa que le ayuda a verificar la identidad de un comprador en línea en tiempo real con una clave privada. Este programa brinda a los clientes una capa adicional de seguridad para que puedan comprar en línea con confianza. Tanto los consumidores como los comerciantes se benefician del uso de este sistema. Los comerciantes verán menos contracargos por transacciones no reconocidas e intentos de fraude de transacciones en línea.

Para el consumidor, no se necesita registrarse para obtener una nueva tarjeta para registrarse en el programa Pagos seguros de Visa. Los tarjetahabientes pueden solicitar a su institución financiera que se vincule la tarjeta a Verified by Visa y les proporcione un código de seguridad, o pueden unirse al programa al mismo tiempo que la compra, ya que Verified by Visa los redirigirá a su propio sitio web para crear su Clave propia. Tan pronto como los consumidores tienen llaves de seguridad, podrá pagar con una visa.

2.3.4.7. Protocolo HTTPS (protocolo de Transferencia de Hiper-Texto).

Según Ryte (2021) el protocolo HTTPS es quien permite establecer una conexión segura entre el servidor y el cliente a la que no puede ser interceptada por personas no autorizadas. En resumen, es una versión segura del Protocolo de Transferencia de Hipertexto (http). Las conexiones HTTP estándar en Internet pueden ser fácilmente interceptadas por terceros. El propósito de una conexión HTTPS es evitar que esto suceda: cifrar sus datos para una transmisión segura de datos. La transmisión está encriptada y el servidor está autenticado.

Cuando el usuario hace clic en el enlace o confirma la entrada de URL en la barra de direcciones con la tecla Intro, el navegador se conecta. El servidor proporciona un certificado de que es un proveedor auténtico y de confianza. Después de la autenticación, el cliente envía una clave de sesión que solo el servidor puede leer. El cifrado ahora se puede realizar en función de esta información crítica. Comúnmente se usa un certificado SSL.

2.3.5. Mecanismos de seguridad

Para proporcionar seguridad al momento de realizar una transaccione en línea según Parrilla (2015) menciona que no existe un único mecanismo capaz de proveer todos los servicios anteriormente citados, pero la mayoría de ellos hacen uso de técnicas criptográficas basadas en el cifrado de la información, los más importantes son las que vamos a mencionar:

El intercambio de autenticación: confirma que la información deseada sea llegada al receptor, por ejemplo, A envía un número aleatorio encriptado con la clave pública de B, B descifra con su clave privada y se lo envía a A, demostrando así

que fue él quien dice ser. Eso sí, hay que tener cuidado al desarrollar estos protocolos porque hay ataques que pueden romperlos. A si mismo tenemos el cifrado de datos que es una de las medidas de seguridad más importantes en las transacciones en línea, ya que garantiza que ninguna persona, organización o proceso no autorizado pueda leer la información. El texto sin formato o como lo denominamos texto simple se convierte en texto de código o un texto cifrado.

De la misma manera la integridad de datos es el mecanismo de seguridad encargado de codificar una secuencia comprimida de datos para su transmisión, la cual es comúnmente conocida como valor de verificación de integridad (ICV). Este mensaje se envía al destinatario con la información habitual. El receptor repite la compresión y luego encripta los datos y compara el resultado con el resultado recibido para asegurarse de que los datos no hayan sido alterados.

Otro mecanismo muy importante a mencionar es el denominado mecanismo de firma digital, que encripta la secuencia de datos comprimidos para su transmisión con la clave privada del remitente. La firma electrónica se envía con la información habitual. Este mensaje es procesado por el receptor para comprobar su integridad, desempeña un papel importante en la disponibilidad del servicio.

El control de acceso, uno de los mecanismos más comunes pero muy necesarios en las transacciones en línea, intenta garantizar que solo los usuarios autorizados puedan acceder a los recursos del sistema como también a los servicios de esta, dando como un claro ejemplo a las contraseñas de acceso. Que podrá obtener acceso la persona que tenga la contraseña.

Un mecanismo a conocer su funcionamiento es el control de encaminamiento o de ruta la cual permite enviar información a través de áreas específicas que deben mantenerse privadas. Además, permite solicitar otras rutas en caso de violación de integridad persistente en una de las rutas.

El mecanismo de seguridad de la red y uno de los mecanismos reconocidos por la sociedad es el firewall, que se considera como el guardián de la seguridad de Internet para la empresa, sin una configuración adecuada y un despliegue estratégico, no se puede garantizar la seguridad de la red empresarial. A medida que

crece su negocio en línea, su firewall se convierte en la parte más importante para proteger su perímetro del acceso no autorizado.

Tabla 1

Mecanismos de seguridad de la información

Mecanismo	Descripción	Características	Ventajas
Firmas digitales	Es un conjunto de datos en forma electrónica, asociados a otros que pueden ser utilizados como medio de identificación del firmante.	• Identifica de forma inequívoca al firmante. • Asegura la integridad del documento firmado. • Garantiza el no repudio	• Facilita las operaciones que se desarrollan por medio de plataformas digitales. • Garantiza la autenticidad del documento. • Garantiza que el documento no ha sido modificado
Certificados Digitales	Es el único medio que permite garantizar técnica y legalmente la identidad de una persona en internet. Es un requisito obligatorio para que las instituciones puedan ofrecer servicios por internet.	• Permite cifrar las firmas digitales. • Consta de una pareja de claves criptográficas, una pública y una privada.	• Da la garantía de que el documento no ha sido manipulado. • El firmante no podrá negar la autoría del documento. • Únicamente el destinatario puede abrir el documento.
Cifrado	Es un procedimiento de seguridad que consiste en alterar los datos que componen un archivo, de tal modo que se vuelvan ilegibles en caso de que sean interceptados por un tercero.	• Criptografía simétrica: se usa en el uso de una única clave para cifrar y descifrar el documento. • Criptografía asimétrica: la clave debe ser enviada al receptor por medio de un canal digital.	• Evita el manejo inapropiado de la información. • Se minimiza el riesgo de manipulación y robo de la información. • Blinda las comunicaciones de una organización

SSL	Es un estándar de seguridad que permite la transferencia de datos cifrados entre un navegador y un servidor web.	• Auténtica la seguridad del sitio web. • Cifra la información transmitida	• Garantiza a los usuarios que el sitio web que visitan es seguro. • Disminuye el riesgo de manipulación de la información.
Firewalls	Es un elemento informático que trata de bloquear el acceso a una red privada a personas que no han sido autorizadas.	• Firewall de hardware: se halla instalado en el Reuter que se usa para entrar a internet, protege los ordenadores de la red. • Firewall de software: viene con el sistema operativo del ordenador y solamente protege el equipo.	• Protege las redes informáticas de usuarios no autorizados. • Preserva la seguridad y privacidad de los navegantes.

Nota: Esta tabla muestra los mecanismos de seguridad de información que son necesarios para una transacción en línea segura.

Según Sabogal (2021) cada mecanismo enumerado y comparado anteriormente tiene diferentes características, propiedades, ventajas y desventajas, y una combinación de dos o más mecanismos garantiza la seguridad completa de su información confidencial, tanto del vendedor como del comprador. Según varios expertos, los firewalls son el mecanismo de seguridad más utilizado porque combinan múltiples mecanismos de seguridad y brindan un mayor nivel de confianza y seguridad. Además de los mecanismos mencionados anteriormente, es importante tener en cuenta los principios de garantizar la seguridad de las transacciones en línea y estas son:

- Principio de confidencialidad
- Principio de integridad
- Principio de accesibilidad

Tabla 2

Principios que garantizan la seguridad de las transacciones en línea

Principio	Descripción	Características
Principio de confidencialidad	Se refiere a los esfuerzos de una organización para mantener sus datos privados	• Controla el acceso a los datos para mantenerlos privados. • La clasificación de datos y controles de acceso disminuye el riesgo
Principio de integridad	Indica que la información con la que se trabaja debe ser concisa y precisa, casi exacta. Tanto en el contenido como en los procedimientos involucrados	• Da la certeza de que la información no ha sido manipulada
Principio de accesibilidad	Indica que la información debe estar disponible siempre que el usuario tenga que consultarla.	• Permite al usuario el uso y consulta la información cada vez que lo requiera. • Da la seguridad de que la información no ha sido modificada por terceros

Nota: Esta tabla muestra los principios que garantizan la seguridad de las transacciones en línea.

2.3.6. Pasarelas de pagos

Las pasarelas de pago son sistemas de pago electrónico que permiten realizar pagos y transferencias seguras entre tiendas electrónicas y bancos utilizando protocolos criptográficos. En pocas palabras y fáciles de comprender cifra la información confidencial entre el vendedor y el comprador para mantenerla segura. Todas las pasarelas de pago cobran una tarifa por cada transacción completada y están equipadas con sistemas de seguridad de comercio electrónico para evitar fraudes.

Actores que intervienen en las pasarelas de pago

Según Manotoa (2021) en las pasarelas de pago intervienen los siguientes: El cliente quien es el que tiene la tarjeta de crédito o débito y quiere acceder a los productos o servicios vendidos por el comercio que realizó la transacción. Banco emisor es quien emite una tarjeta de crédito o débito en nombre del cliente o titular de la tarjeta y en nombre de las compañías de tarjetas de crédito o débito como Visa o MasterCard. Además, tenemos al Comerciante que viene a ser una empresa o empresas en línea que fabrica u ofrece todo tipo de servicios a sus clientes.
Banco beneficiario: esta es la institución financiera que mantiene la cuenta bancaria del comerciante la cual envía la transacción del vendedor al banco emisor para el pago. Como puede ver, sin los participantes descritos anteriormente, las transacciones financieras a través de dispositivos electrónicos no serían efectuadas y en donde la pasarela de pago actúa como intermediario.

Cómo funciona una pasarela de pago

Según Cárdenas & Petro (2022) una pasarela de pagos funciona como un proceso en el que se realiza la compra y venta de bienes o servicios en línea, con algunas entidades, hasta llegar a un resultado final que viene a ser el resultado el pago realizado por la compra en línea para entenderlo más detalladamente vamos a describir el proceso que se lleva a cabo y como procede la paradera de pago en todo esto. Por un lado, encontramos al vendedor, al comprador y al banco emisor. Por otro lado, encontramos las pasarelas de pago, que son sistemas o software que utiliza la empresa para su comercio electrónico; banco comprador significa el banco receptor de las transacciones electrónicas a recibir; el procesador de pagos es el vínculo entre el emisor de la tarjeta utilizada como medio de pago y el banco autorizado del comerciante; finalmente el sistema de tarjeta del cliente, es decir, la red de pago a la que pertenece la tarjeta. Dependiendo de la ubicación del cliente, determinará a qué banco corresponde la tarjeta. A continuación, se detallan los siguientes procesos:

1. El comprador selecciona uno o más productos, los coloca en el carrito de compras, hace clic en el botón "Comprar" e ingresa los detalles de pago en el formulario de pago (datos de la tarjeta, cuenta de PayPal, etc.).

2. Después de hacer clic en el botón "Pago", la información de pago se envía a la pasarela de pago en forma encriptada utilizando los protocolos SSL (Secure Sockets Layer) o TLS (Transport Layer Security).
3. La pasarela de pago envía la información al procesador de pago, que transfiere la información al sistema de tarjeta del cliente (VISA, MasterCard, American Express, etc.).
4. El sistema de tarjetas realiza una serie de comprobaciones con el banco emisor del cliente para verificar si la información proporcionada es correcta, si tiene fondos suficientes. Además, el banco emisor ahora es responsable de exigir una autenticación sólida del cliente cuando así lo exijan las reglamentaciones de PSD2.
5. Los resultados de la verificación se envían al sistema de tarjetas, los procesadores de pago y las pasarelas de pago informan los resultados a los compradores y vendedores.

Al final todo el proceso, que a primera vista parece largo y complicado, lleva solo 3 segundos, mientras que la compra simultánea se realiza en la tienda online.

2.3.7. Empresas que brindan el servicio de Pasarelas de pagos en el Ecuador

En el Ecuador existen proveedores de servicios de pago electrónico o sistemas auxiliares de pago, que funcionan como una extensión de los servicios del Banco Central del Ecuador, se les conoce como pasarelas de pago y se encuentran al servicio en todo el territorio nacional.

Según el Código Orgánico Monetario y Financiero Registro Oficial Suplemento 332 en el Articulo 105 afirma que los sistemas auxiliares de pago son el conjunto de políticas, normas, instrumentos, procedimientos y servicios articulados y coordinados, públicos o privados, autorizados por el Banco Central del Ecuador, interconectados con el sistema central de pagos, establecidos para efectuar transferencias de recursos y compensación entre sus distintos participantes.

Las entidades administradoras de los sistemas auxiliares de pago (pasarelas de pago) son entidades del sistema financiero autorizadas por el Banco Central del Ecuador para efectuar transferencias de recursos monetarios o compensaciones entre sus participantes. Adicionalmente, se consideran ASAP las empresas

autorizadas por la Superintendencia de Compañías, Valores y Seguros para efectuar actividades de remesas de dinero.

Las entidades Administradoras de los sistemas auxiliares de pago autorizadas por el Banco central del Ecuador para brindar el servicio de pasarelas de pago son los siguientes:

Tabla 3

Entidades autorizadas como administradoras de los sistemas auxiliares de pago

Nro.	Código	Nombre de la entidad	Nro. Resolución	Fecha de resolución	Servicio autorizado
1	0044	Alignetsa S.A.	BCE-DNRO-2022-024	2022-06-08	Pasarela de pagos
2	0052	Cardtech Ecuatoriana S.A.	BCE-DNRO-2022-031	2022-06-08	Pasarela de pagos
3	0030	Ecuapayphone C.A.	BCE-DNRO-2022-039	2022-06-08	Pasarela de pagos
4	0034	Kushki S.A.	BCE-DNRO-2022-043	2022-06-08	Pasarela de pagos
5	0058	PagoPlux S.A.	BCE-DNRO-2022-051	2022-06-08	Pasarela de pagos
6	0054	Paymentez (Nuvei)	BCE-DNRO-2022-057	2022-06-08	Pasarela de pagos
7	0062	PlaceToPay	BCE-DNRO-2022-059	2022-06-08	Pasarela de pagos

Nota: Esta tabla muestra las entidades administradoras de los sistemas auxiliares de pago autorizadas por el Banco central del Ecuador.

Las entidades administradoras de los sistemas auxiliares de pago que se muestran en el gráfico, en esta investigación se denomirán como pasarelas de pago, es decir, entidades que se unen a los intermediarios para realizar transferencias en línea, con la garantía de que su eficacia coincide con la seguridad que brindan. Ahora bien,

vamos a ir detallando cada una de estas entidades para conocer cuál es su rol en las transacciones en línea en el Ecuador. Cabe mencionar que las pasarelas de pago mencionadas a continuación son entidades ecuatorianas y que se encuentran avaladas por el banco central de ecuador.

2.3.7.1. Alignetsa S. A.

Una empresa dedicada a brindar soluciones tecnológicas y de seguridad para el sector del comercio electrónico y pagos seguros. Alignet (2022) señala que la empresa demuestra que enfoca todo su conocimiento para brindar soluciones innovadoras para el creciente mercado del comercio electrónico en el Ecuador. Es pionera en Latinoamérica en lanzar la solución de autenticación de seguridad EMV 3D Secure (3D Secure 2.0) para soportar Visa y MasterCard Identity Check (MaterCard SecureCode).

Desde 2002, Alignet ha ampliado los servicios de procesamiento de autenticación tanto para emisores como para compradores a varios países de la región, como lo son Costa Rica, Panamá, Guatemala, Uruguay, Chile, México, Bolivia y Colombia, siendo así considerado en la actualidad como una de las principales empresas proveedoras de soluciones para los principales bancos emisores y adquirentes de América Latina.

Gracias a su amplio conocimiento de productos en diversos mercados y la experiencia exitosa de proyectos prácticos, Alignet tiene en su cartera de clientes a más de 40 instituciones financieras entre bancos emisores, entidades adquirentes y procesadoras de pagos, que ya les atiende regularmente en 11 países la cual representa su importancia dentro del comercio electrónico y sobre todo al momento de realizar pagos en línea.

Según Alignet (2022) en su página oficial establece los siguientes estándares de seguridad:

Autenticación 3-D Secure 2.1

Verificado por Visa y MasterCard, los protocolos de seguridad SecureCode ayudan a los comerciantes a verificar que el titular de la tarjeta es quien está realizando una

compra. Protocolo de suma importancia a la hora de verificación y validación de información del usuario. A sí mismo el monitoreo antifraude que realiza un rastreo exhaustivo a fin de que se prevenga el fraude en línea, detectando transacciones sospechosas de manera oportuna y reduciendo el riesgo de robo de identidad.

También cuenta con la certificación PCI DSS, otorgada solo a organizaciones que cumplen con los estándares de seguridad de la industria de tarjetas, lo que garantiza la protección y la integridad de los datos del cliente. Y como no mencionar al Cifrado TLS 1.2 que se hace presencia al momento que los datos enviados por el cliente se cifran con el protocolo de seguridad TLS 1.2 (socket de capa de transporte) para proteger la confidencialidad de la información

2.3.7.2. Cardtech Ecuatoriana S.A.

Como nos menciona Cardtech (2021) en su página oficial donde nos da a conocer que son una organización internacional de capital privado con más de veinte años de experiencia brindando soluciones para pagos, seguridad de acceso e interacción digital y sobre todo en la confidencialidad en el tratamiento de la información buscando de esta manera la satisfacción del cliente a través de un programa de excelencia, Las certificaciones que poseen son una demostración de compromiso con los clientes demostrando así la calidad y la seguridad en todos los niveles.

Estándares de seguridad

Políticas del Sistema Integrado de Gestión (SIG)

La gerencia de Cardtech Ecuatoriana, filial del sistema financiero que ofrece la personalización de tarjetas financieras, alquiler y venta de cajeros automáticos (ATMs), reconoce la importancia de la calidad y de seguridad de la información, que se enfoca en el desarrollo integral, las políticas del sistema integrado de gestión SIG la detallamos en el siguiente apartado:

Satisfacer de forma segura y sostenible las expectativas, necesidades y oportunidades de crecimiento de los clientes adaptándonos a los nuevos requerimientos del mercado y sobre todo manteniendo altos estándares de calidad.

Contribuir continuamente a la mejora absoluta de la eficacia y eficiencia del Sistema Integrado de Gestión, proporcionando los recursos necesarios para implementar y fortalecer el SIG. Para garantizar la confidencialidad, integridad y disponibilidad de la información del cliente y de la organización según lo requieran cumpla estrictamente con los requisitos legales aplicables a SIG.

Esta política se ha redactado de acuerdo con el propósito y al contexto de la organización para respaldar la dirección estratégica, exactamente como se presenta en consulta con los empleados en un escenario de mejora continua para el fácil y seguro uso de los servicios de la pasarela de pago ante los clientes.

Además, la pasarela también cuenta con la certificación ISO 27001 Sistemas de gestión de seguridad de la información. Según la Agencia Nacional de Gestión de Calidad (NQA, 2013), ISO 27001 (Organización internacional para la estandarización) es un estándar internacional que proporciona un marco para un Sistema de gestión de seguridad de la información (SGSI). Con la finalidad de brindar la confidencialidad, integridad y disponibilidad continua de la información, así como el cumplimiento legal. La certificación ISO 27001 es esencial para proteger sus activos más importantes como la información de clientes y empleados, la imagen de la empresa y otros datos importantes.

La implementación de ISO 27001 es una respuesta perfecta a los requisitos legales y de los clientes, incluida el Reglamento general de protección de datos (GDPR) y otras amenazas potenciales que incluyen: delitos informáticos, violaciones de identidad, vandalismo/terrorismo, uso malicioso, robo y ataques de virus.

2.3.7.3. Ecuapayphone C.A.

Es una empresa registrada bajo las leyes de la República del Ecuador, autorizada para prestar servicios al sistema financiero de conformidad con lo dispuesto en el Código Orgánico Monetario y Financiero, operando principalmente bajo la razón social Payphone.

Según Castro (2017) EcuaPayPhone se fundó en mayo del 2014 como una sociedad de 3 ingenieros ecuatorianos con amplia experiencia en el desarrollo de aplicaciones

móviles, quienes lograron identificaron la necesidad de utilizar los teléfonos inteligentes como medio de pago. El resultado fue PayPhone, una aplicación móvil que le permite realizar transacciones en línea desde su teléfono inteligente simplemente registrando la tarjeta con el número de teléfono móvil del propietario, implementa el concepto por el cual se requieren dos elementos para el pago: una tarjeta de crédito y un terminal de punto de ventea (TPV) y la aplicación reemplaza el uso real de una tarjeta de crédito por parte del usuario durante el procesamiento del pago.

En el año 2015, PayPhone recibió la certificación internacional Visa y luego la certificación internacional MasterCard, lo que llamó la atención del equipo de Promerica-Produbanco, que apoyó el proyecto y ahora ofrece como parte del proyecto una amplia gama de servicios financieros. Además, PayPhone está certificado por el Banco Central del Ecuador para el uso de criptomonedas.

En el mismo año en el Banco Digital de Colombia, PayPhone recibió por primera vez el reconocimiento internacional, donde 22 empresarios latinoamericanos presentaron diferentes plataformas con innovadoras soluciones tecnológicas para la industria financiera. Como resultado, el jurado decidió que PayPhone (Ecuador) es la mejor plataforma.

Como dato adicional mencionar que la aplicación PayPhone se encuentra disponible para tarjetas de crédito Produbanco Visa y MasterCard y para smartphones con sistemas operativos Android, iOS y Windows Phone.

Los pasos a seguir de cómo utilizar la pasarela de pago es:

Como primer paso debemos descargar la aplicación, ya con la aplicación descargada vamos a crear un usuario en la cual vamos a registrar nuestra clave de acceso para la aplicación. Luego ingresaremos los datos personales y los verificaremos según lo requiera el sistema.

Seguidamente anotamos el número de tarjeta de crédito o débito y el código de seguridad CVV que la podemos encontrar en el reverso de la tarjeta. Si los datos

ingresados y registrados son correctos, se activa el servicio para que el usuario pueda realizar compras en los establecimientos afiliados.

Para tramitar el pago, el usuario solo necesita proporcionar el número de móvil y la aplicación le notificará el consumo y le solicitará el código de acceso a la aplicación. Luego se selecciona la tarjeta con la que desea realizar el pago y el sistema enviará un mensaje de autorización al punto de venta y se realiza el pago.

En materia de seguridad al momento de realizar el pago a través de la transferencia en línea, PayPhone garantiza y resguarda la información de la tarjeta de los usuarios debido a que funciona bajo el estándar de seguridad PCI DSS el cual permite encriptar todos los datos enviados durante la transacción. El usuario solo facilita el número de teléfono móvil y nunca los datos de su tarjeta de crédito. Además, cada transacción requiere de una contraseña la cual es generada por el usuario y por ende debe coincidir con el código de usuario de PayPhone.

Estándares de seguridad

Motor antifraude SEON

También es importante reiterar que la pasarela de pago Payphone cuenta con un mecanismo antifraude SEON, revelado por SEON Technologies (2022) establece que combate el fraude en tiempo real utilizando herramientas avanzadas de SEON para ayudarlo a administrar su propio negocio en línea.

Mencionar que SEON realiza auditorías en tiempo real en más de 50 plataformas digitales y sociales con la finalidad de clasificar entre los clientes y personas terceras como pueden ser estafadores, filtrando a los estafadores antes de las costosas comprobaciones de KYC y de identificación puesto que descubre fácilmente a los usuarios que comparten dispositivos y configuraciones similares para señalar a los reincidentes y detener las redes de fraude en su camino. La gestión de riesgos flexible y las API modulares de SEON funcionan con los sistemas existentes para mejorar la protección.

Control de transacciones

Erazo & Montenegro (2005) el sistema de gestión de transacciones es el encargado de gestionar, controlar y transmitir información sobre las transacciones.

2.3.7.4. Kushki S.A.

Según Manotoa (2021) es una sociedad constituida bajo las leyes de la República del Ecuador cuyo objeto social es la prestación de servicios financieros auxiliares, la plataforma integra soluciones tecnológicas que permite, a través de convenios o alianzas, licenciar software a una determinada red de afiliados.

Sus servicios incluyen en procesamiento de pagos en tiempo real y redes sociales; proporcionar un enlace de pago; pagos recurrentes; mobile bill and pay box que combinan los métodos anteriores: coopera con todas las instituciones bancarias del país, incluidas comercio electrónico, comercio móvil y los canales comerciales. La pasarela de pago Kushli S.A. amplía su capacidad de realizar transacciones en un entorno digital, el costo es bajo en comparación con las transacciones en efectivo y también permite satisfacer las necesidades de cobro de deudas de sus clientes. Tenga en cuenta que no procesa pagos con tarjetas internacionales.

Estándares de seguridad

Según Kushki (2018) señala que cuentan con la mejor tecnología para proteger datos sensibles y prevenir fraudes. Ofreciendo 3 niveles de seguridad.

Nivel 1 Seguridad en el manejo y transmisión de datos sensibles

PCI DSS Nivel 1

Cuentan con el certificado de seguridad más alto en el mercado debido a que se procesa una gran cantidad de transacciones en línea y a los que se les aplica el 100% de los controles del estándar de PCI DSS, mostrando así a los usuarios experiencia y confiabilidad en la pasarela de pago. También dispone de tokens para proteger los datos de las tarjetas de crédito, evitando que los estafadores roben y utilicen información confidencial al convertir el número de tarjeta en un código con caracteres aleatorios (token).

También cuenta con seguridad Bóveda Nivel 1, donde la seguridad es primordial ya que es el único lugar donde se almacenan los datos de las tarjetas de los consumidores. La interfaz unificada de Kushki proporciona un control estricto de la información y cumple con PCI para máxima seguridad.

Nivel 2: Prevención de fraude

En el nivel de seguridad 2 que brinda la pasarela de pago está relacionada con la prevención contra los posibles fraudes, analizada trabajando en tiempo real para identificar señales de advertencia para poder prevenirlos.

Para mayor eficiencia, la pasarela de pago cuenta con un motor de aprendizaje automático (Machine Learning) que se encuentra respaldado por la red global más grande de la industria, el sistema toma decisiones en milisegundos seguidamente analiza los patrones de comportamiento detectando anomalías no intuitivas y sobre todo bloqueando transacciones de alto riesgo.

Puntaje transaccional

Usando el reconocimiento de patrones y las reglas de seguridad, clasifican las transacciones por nivel de riesgo, lo que le permite identificar clientes reales y cumplir con los pedidos con mayor confianza.

Nivel 3: Autenticación y verificación

Para entender el funcionamiento del nivel 3 correspondiente a la autenticación de doble factor primeramente se verifica y valida al cliente para que la compra se realice de forma segura. Para ello, se realiza un micro pago mediante un código de autenticación que el cliente deberá introducir en la web para formalizar la compra.

2.3.7.5. PagoPlux S.A.

Esta es una empresa ecuatoriana que participa en actividades financieras y de inversión. Es una plataforma de pago omnicanal para empresas y comercios facilitando en los pagos fáciles, rápidos y sobre todo seguros.

Según PagoPlux (2022) los pagos realizados a través de la pasarela de pagos señalan que son más seguros y confiables debió a que cumple con las reglas y el estándar

requerido para brindar servicios de botón de pago, la cual ah recibió una revisión positiva por parte de la Superintendencia Bancaria para formar parte de los denominados asistentes financieros.

Ademas Kruger (2021) menciona que ser productivos al momento de facilitar en los pagos a los usuarios genera y promueve estrategias que permitan a más personas a formar parte de la pasarela de pago y poder satisfacer las necesidades de las personas al momento de realizar una transacción en línea. Puesto que gracias a herramientas como PagoPlux se puede integrar botones de pago a las páginas Web sin tener que invertir mucho tiempo.

Esta nueva herramienta, que se ha desplegado rápidamente en el mercado ecuatoriano, ofrece una variedad de beneficios, uno de los cuales es la seguridad, ya que es respaldada por las instituciones financieras más importantes del país que a su vez garantiza a los usuarios una total tranquilidad al momento de realizar los pagos a través de las transacciones en línea.

Pero esto no termina ahí además la plataforma de pago PagoPlux ofrece una experiencia de compra moderna para que puedas convencer a los clientes de formar parte de ello a si mismo cuentan con diseño de sitio web moderno y profesional, así como servicios como pagos recurrentes, pagos con código QR y más. Y ya para finalizar cabe mencionar una de las características que hacen de PagoPlux sea un gran aliado para los desarrolladores y es que se integra fácilmente con los sitios web y redes sociales de los clientes y sobre todo no se requiere codificación para su implementación.

Estándares de seguridad

Validación One Time Password (OTP)

Según Sifone (2002) la validación OTP brinda máxima seguridad para contratos, transacciones y/o comercio electrónico. Una herramienta de autenticación de dos factores que puede generar un código OTP por teléfono utilizando el número de teléfono móvil de su cliente como token.

Los beneficios proporcionados por OTP son las siguientes:

Esta solución es mucho más económica que los tokens físicos y más confiable y eficiente que las soluciones basadas en SMS. Si bien es completamente imposible conocer la identidad del usuario que utiliza el pase o recibe el MSJ vía SMS, el sistema de control de la OTP registra evidencias de cada uso.

El factor de autenticación es capaz de identificar biométricamente a las personas con una huella digital de voz, que es tan segura como una huella digital y proporciona la misma prueba de los procesos realizados. La verificación OTP permite identificar a los usuarios del sistema a través de la autenticación, una función que otros sistemas de verificación de transacciones no pueden realizar.

Motor antifraude ACI ReD Shield

Según Aciworldwide (2021) el motor antifraude de Red Shield ACT ofrece soluciones rápidas y precisas para transacciones en línea y móviles en todas las regiones y formas de pago. Esta solución extremadamente flexible y combina varias capas de controles para adaptar su estrategia de prevención del fraude. Los modelos avanzados de aprendizaje automático como lo es el análisis predictivo y de comportamiento además las técnicas de creación de perfiles de clientes, las reglas personalizadas y el análisis de fraude global se combinan para identificar transacciones reales de las fraudulentas.

Se basa en un análisis integral de fraude comercial y combina datos críticos de asociaciones globales con información de socios y otros terceros, así como datos de mercado negativos y datos fundamentales de mercados verticales. Los especialistas en marketing utilizan esta información para crear mejores perfiles de clientes, identificar nuevas tendencias de fraude y sobre todo mejorar el rendimiento de nuestros modelos de aprendizaje automático en la tomar medidas inmediatas para evitar pérdidas por fraude.

Nuestra detección retrospectiva también permite la puntuación de pedidos en tiempo real lo que significa que bloquea la actividad fraudulenta en varias etapas del ciclo de transacción, evitando pérdidas y sobre todo cierra el fraude más rápido.

Verificación de Correo electrónico

Según Validity (2021) la verificación y validación de correo electrónico garantiza que las direcciones de correo electrónico sean reales antes de enviarlas, lo que le ahorra tiempo, dinero y recursos de direcciones de correo electrónico falsas. La verificación de correo electrónico reduce el riesgo de altas tasas de rebote, trampas de spam y listas negras que pueden afectar negativamente su reputación y tráfico de red. Estos factores también pueden costarle dinero, ya que los costos de adquisición perdidos y el menor valor de vida útil del cliente (CLV) equivalen a un retorno de la inversión (ROI) reducido.

Algunos de los métodos más comunes para verificar nuevas direcciones de correo electrónico incluyen verificar la suscripción (doble suscripción o DOI) y crear pautas. Sin embargo, cada uno de estos enfoques tiene inconvenientes: el registro DOI lleva más tiempo y los clientes no pueden hacer clic en el enlace de confirmación. En promedio, el 25 % de los suscriptores pasan el proceso DOI, lo que puede resultar en una alta pérdida de ingresos.

Verificación de identidad KYC (Know Your Customer)

Según Electronic IDentification (2022) los principios KYC (Know Your Customer) se basan en el proceso de identificación y verificación del cliente, el uso de diversos controles y verificaciones para evitar hacer negocios con personas asociadas con el terrorismo y la corrupción. o lavado de dinero entre otros. Por tanto, se trata de verificar que los clientes son quienes dicen ser, dándoles así la propiedad y el acceso a los servicios o productos que alquilan ya los que quieren tener acceso. Esta verificación se lleva a cabo por varios métodos.

Los diferentes organismos reguladores tienen diferentes requisitos. Algunos incluyen:

- Carnet de conducir
- Pasaporte
- Prueba de dirección del documento

El proceso Know Your Customer se puede llevar a cabo de forma tanto online como presencial.

2.3.7.6. Paymentez (Nuvei).

Es una empresa que brinda a compradores y empresas una solución completa para pagos en línea seguros, rápidos y fáciles de usar. Lleva en el mercado alrededor de 10 años y cuenta con más de 5 millones de clientes.

Dedicada a los pagos online que procesa pagos de sitios de comercio electrónico ecuatorianos y está vinculado a adquirentes locales, específicamente de tarjetas de crédito, ello facilita poder pagar de manera diferida o rotativa, además acepta tarjeta de débitos y prepago.

Según GlobeNewswire (2021) fundada en 2011, Paymentez brinda a las instituciones financieras y comerciantes una amplia gama de soluciones de pago, que incluyen pasarela de pago, marca blanca, adquisición de tarjetas y opciones de tarjetas prepagas. Paymentez admite verticales de comercio electrónico de rápido crecimiento que incluyen juegos en línea, plataformas de entrega, movilidad, transporte, deportes y más en América Latina.

Paymentez ofrece conexiones directas en 11 países y entrega local en 9 países (México, Ecuador, Venezuela, Colombia, Brasil, Perú, Argentina, Uruguay y Chile). Además, acepta más de 80 métodos de pago locales y alternativos, como transferencias bancarias, monederos electrónicos, redes de pago instantáneo, redes de efectivo más relevantes y otros. Por lo tanto, proporciona una plataforma de pago local completa a más de 4.000 comercios en la región.

Nuestra presencia, experiencia, conectividad y conocimientos en América Latina, combinados con la tecnología, el rápido crecimiento y el liderazgo de Nuvei, crean la plataforma de pagos líder en la región. Nuestros clientes disponen una plataforma de clase mundial con la mejor conectividad y soporte de la región. El futuro es muy ilusionante", Juan F. Franco, recientemente nombrado Gerente General de Nuvei Latinoamérica.

Acerca de Nuvei

Somos socio de tecnología de pagos de las exitosas marcas Nuvei (TSX: NVEI and NVEI.U). Ayudamos a las empresas a crecer más rápido mediante la integración de inteligencia y la tecnología que necesitan para tener éxito a nivel local y global.

Al combinar la tecnología de pago y el asesoramiento relacionado, ayudamos a las empresas a eliminar las barreras de pago, optimizar los costos operativos y aumentar las tasas de adopción. Nuestra plataforma patentada brinda opciones transparentes de pago y cobro que conectan a los comerciantes con los clientes en 204 mercados globales y compras locales en 45 mercados. Con soporte para más de 480 métodos de pago nativos y alternativos, casi 150 monedas y 40 criptodivisas, los comerciantes pueden aprovechar cualquier oportunidad de pago que surja. Nuestro objetivo es hacer de nuestro mundo un mercado local.

Estándares de seguridad

Según Nuvei (2022) en su página oficial brinda información sobre soluciones de cumplimiento y seguridad, y cómo mantiene las transacciones seguras:

Tecnología EMV (Tarjeta con chip)

EMV es un estándar global para reemplazar la tarjeta de cinta magnética, es diseñado para procesamiento de tarjetas de débito y crédito. La tecnología inteligente de chips también se conoce como chip, PIN o chips y firmas que consisten en microprocesadores integrados con tarjetas de débito y dispositivos inteligentes (como teléfonos móviles).

Evite la responsabilidad por transacciones fraudulentas mediante la adopción de una solución compatible con EMV. Somos los primeros en ofrecer soluciones habilitadas para EMV para brindar una mejor protección contra actividades fraudulentas. Nuestras soluciones de terminales de punto de venta permiten pagos más rápidos y una mayor seguridad. Acepte tarjetas de contacto y sin contacto con dispositivos de pago innovadores y preparados para el futuro en la tienda y sobre la marcha.

Cifrado punto a punto (P2PE)

Con la plataforma P2PE certificada de Nuvei, las empresas pueden sentirse seguras de haber reforzado su seguridad y el punto de venta. Hemos agregado protección de datos del titular de la tarjeta de nivel superior. Además de brindar sólidas medidas antifraude, nuestra solución P2PE reduce efectivamente el alcance de PCI DSS para comerciantes, ISV y VAR, lo que reduce el costo y el esfuerzo necesarios para lograr y mantener el cumplimiento.

Detección de fraude integrada

Los pagos más seguros e inteligentes están aquí. Nuestra plataforma de toma de decisiones avanzada ayuda a prevenir el fraude en línea antes de que suceda. Lo mejor de todo es que está integrado directamente en nuestra pasarela de pago, no se requiere una solución de terceros.

- Rastrea y monitorea la actividad del cliente a través de todo el sitio a través de múltiples dispositivos.
- Segundos después de un pago, se otorga una puntuación de riesgo a cada transacción para determinar la probabilidad de fraude.
- Funciona completamente en segundo plano y no interferirá con la experiencia de compra del cliente.

Tokenización

La tokenización es un método de seguridad de datos que reemplaza la información de la tarjeta de crédito con un token, un valor aleatorio que almacena información básica de la tarjeta sin comprometer la seguridad. La tecnología de tokenización de Nuvei permite el acceso a los datos de facturación sin necesidad de almacenar la información de la tarjeta de crédito. Esto es especialmente útil para fines de suscripción o facturación recurrente.

Cada token está vinculado a un único perfil de cliente y se puede utilizar para completar una transacción de compra. Los comerciantes pueden procesar

transacciones de forma segura y reducir el riesgo de que los datos confidenciales caigan en manos equivocadas. La seguridad adicional permite a las empresas ahorrar tiempo y dinero en comparación con la integración con soluciones de terceros.

EKYC y gestión de identidad

Proteja su negocio contra el fraude con nuestro Administrador de identidad mientras incorpora clientes de forma rápida y sencilla. Manténgase al día con los últimos requisitos de cumplimiento normativo en todo el mundo. Nuestras verificaciones de verificación de documentos y eKYC lo ayudan a cumplir con las regulaciones contra el lavado de dinero (AML) mientras cumple con los requisitos de administración de identidad.

Gestión de contracargos

Nuestras soluciones de gestión de contracargos le permiten responder a transacciones con tarjetas no reconocidas y otras disputas potenciales de manera más rápida y efectiva. Acceda a informes detallados a través de nuestro back-office o API, lo que le brinda una visión general clara de la información sobre fraudes

Una devolución de cargo ocurre cuando un cliente se comunica con el banco emisor de una tarjeta de crédito para iniciar un reembolso por una compra que realizó con su tarjeta de crédito. Las razones por las que surgen las devoluciones de cargo pueden variar mucho, pero generalmente son el resultado de que un cliente no está satisfecho con su compra.

Nuestro Tablero de Comerciantes alerta a los dueños de negocios sobre las devoluciones de cargos en caso de que ocurran y ofrece herramientas para ayudar a disputarlos o resolverlos, de manera rápida y eficiente.

También ofrecemos una serie de prácticas recomendadas para evitar las devoluciones de cargo. Después de todo, la mejor manera de lidiar con cualquier contracargo es evitar que suceda.

2.3.7.7. PlaceToPay.

Según Manotoa (2021) PlaceToPay es una empresa que brinda soluciones de pago ágiles y seguras para todo tipo de industria, en múltiples canales, incluso sin tener sitio web. Con una solución de pago, obtiene funciones adicionales a las que puede acceder sin costo adicional.

Funciona en forma de un botón de pagos que permite realizar dicha transacción mediante la autenticación y validación de información, puesto que acompaña al cliente antes, durante y después de realizado este, ya que almacena todas las operaciones. El valor monetario se puede recibir tanto en la cuenta bancaria del comerciante o en su propia plataforma. Este botón juega un papel importante en el comercio electrónico.

Estándares de seguridad

Evertec (2022) menciona que esta sección describe los diferentes módulos de seguridad que ofrece Placetopay dependiendo de los diferentes países en los que se encuentra. No se requiere integración adicional para usar estos módulos de seguridad.

EMV 3-D Secure

Un protocolo internacional para la interoperabilidad entre marcas de tarjetas, emisores y adquirentes para permitir el proceso de autenticación de usuarios para transacciones no presenciales. Esta es una capa adicional de seguridad que ayuda a eliminar los riesgos de pagos no autorizados y protege a los comerciantes del fraude.

3DS Placetopay

Es el servicio que facilita al adquirente enrolar a los comercios y enrutar las transacciones a través del protocolo EMV 3-D Secure, permitiendo realizar el proceso de autenticación del usuario, reduciendo así la exposición de los comercios a los contracargos.

Beneficios

- Al trasladar el riesgo, los comercios pueden explorar nuevas posibilidades para incrementar sus ventas
- Aumenta la competitividad y tendrá un valor agregado adicional, ya que las empresas preferirán un aliado que los proteja.
- Permite a los clientes concentrarse en su negocio y despreocuparse por el riesgo al fraude en transacciones autenticadas.
- Reduce las quejas y pérdidas económicas derivadas de los contracargos en los comercios
- Se incrementarán las tasas de conversión generando mayores ingresos.

AVS

El Servicio de Verificación de Dirección (AVS) es un servicio de prevención de fraude para transacciones sin tarjeta que utilizan la dirección del titular de la tarjeta.

Scudo

Estamos comprometidos con la seguridad, por eso presentamos Scudo, un sistema modular de control de fraude que permite optimizar el costo de las validaciones asegurando un adecuado balance entre la tasa de aprobación y el riesgo de contracargos.

Funcionamiento

La seguridad es prioridad, por eso garantizamos un sistema completo antifraude.

- Cuenta con expertos en seguridad transaccional
- Analiza el historial de pagos de los clientes
- Revisa el historial de pagos en motores de riesgo
- Contrasta información con centrales de riesgo
- Personaliza filtros según las necesidades
- Identifica y bloquea ataques masivos

Beneficios

- Aumenta el nivel de confianza en las transacciones.
- Disminuye los contracargos (reclamación devolución de dinero)
- Facilita la recolección de información para disputar los contracargos.
- Permite realizar el proceso de validación en línea.
- Tendrá un equipo de expertos validando sus transacciones.
- Incrementa la tasa de aprobación de pagos y conversión en su negocio.

Análisis histórico

Este servicio lo incluimos en cualquier plan de procesamiento de transacciones. Consiste en analizar el histórico de compras de los usuarios y esto arroja una calificación de riesgo, que indica si la transacción debe pasar o no por otros módulos de seguridad antes de ser aprobada.

El histórico de compras consiste en el registro que ha dejado el usuario al realizar compras por internet. Se analizan 19 años de historial de transacciones de clientes de todas las empresas afiliadas a PlacetoPay.

Validación en centrales de riesgo

Permite validar si la tarjeta de crédito que están usando para la compra pertenece o no al usuario, a través de una consulta en tiempo real en centrales de riesgo. Además, provee al comercio información adicional como: email, direcciones físicas, teléfonos y números celulares, facilitando al sistema tener mayor certeza en la autenticidad de los datos del usuario pagador.

Validación en motores de riesgo

Este módulo permite realizar la validación de seguridad a través de sistemas de motores de riesgo a nivel mundial, genera evaluaciones de riesgo basadas en el análisis de varias variables relacionadas con el comportamiento de pago del usuario, como historial de compras, ubicación geográfica, huella digital del dispositivo, tipo de conexión a Internet, extradata y muchos otros criterios.

Huella del dispositivo: todas las características que identifican tu dispositivo, como dirección IP, nombre del fabricante, sistema operativo que se utiliza.

Extradata: Información adicional para confirmar la transacción.

Revisión manual

A través de este módulo nuestro equipo experto en seguridad transaccional, analiza los pagos y realiza las validaciones necesarias para garantizar que la transacción sea de bajo riesgo de fraude y pueda ser aprobada.

Manualmente se analiza coincidencia de datos, histórico transaccional y se pueden llevar a realizar llamadas telefónicas para corroborar la identidad de la persona que hace la compra.

2.3.8 Ventajas y desventajas de las pasarelas de pago

Según Cárdenas & Petro (2022) indican que para todo aspecto se manifiestan beneficios y dificultades, este caso no es la excepción, por ello se mencionan las ventajas que tiene tanto para los proveedores, como consumidores y las desventajas en la prestación de este servicio, aunque son menos, que los aspectos positivos que se presentan en el proceso de intercambio para la adquisición de un bien o servicio.

Ventajas

Clientes

- El pago se realiza directamente en los servidores de cada banco.
- El vendedor no maneja información privada del cliente, ya que el número de la tarjeta se introduce en el servidor seguro del banco y se envía encriptado para su comprobación por los emisores de tarjeta, por lo que el vendedor nunca accede a esta información.
- El vendedor debe tener una cuenta abierta en el banco que gestiona la pasarela de pago, por lo que siempre se dispondrá de sus datos legales, minimizando las ventas fraudulentas.
- El cliente puede elegir el tipo de tarjeta a utilizar entre las opciones comerciales. La legislación protege a los consumidores contra cualquier

reclamo pagado con tarjeta de crédito y requiere que los vendedores demuestren quién compró y entregó el artículo.

Vendedor

- Las Terminales Punto de ventas virtuales ofrecen transparencia y seguridad para sus clientes.
- La seguridad de las transacciones realizadas se traslada al banco.
- El cobro de la transacción se realiza en el instante de confirmarse el cargo, siendo el banco el responsable de comprobar la validez de la tarjeta empleada y la disponibilidad de fondos del cliente.
- La rapidez de la venta permite aprovechar la compra impulsiva y la disponibilidad temporal y geográfica, en cualquier lugar del mundo 24/7.
- El sistema de gestión permite hacer un seguimiento de todos los pagos realizados en tiempo real.

Desventajas

Las desventajas afectan principalmente a los vendedores en las cuales se manifiestan las siguientes:

- Las comisiones pueden alcanzar alrededor del 4% de la compra, frente al 2% de las tiendas físicas.
- La gestión de reclamaciones es un tema crítico, ya que debe ser el vendedor el que demuestre la validez de una venta. En estos casos es imprescindible conservar toda la información posible, desde la petición de compra, consultas comerciales, correos de confirmación de pedido, hasta pruebas del envío real de la mercancía vendida, como son los resguardos de las agencias de mensajería

2.3.9. Firmas y certificados digitales

Según Molina (2007) las firmas y certificados digitales se basan en la criptografía, la misma que proviene del griego kryptos, que significa esconder y gráphein, escribir, es decir, escritura escondida. La criptografía se ha utilizado durante muchos años para enviar mensajes secretos diseñados para ser entendidos solo por

personas autorizadas. El sistema de cifrado del software puede ser público o privado.

Los privados requieren para su funcionamiento que el emisor y el receptor posean exactamente los mismos dispositivos, llamados llaves, a fin de codificar y decodificar el mensaje enviado. Si bien el uso de llaves privadas permite alcanzar niveles superiores de seguridad, el problema radica en que utilizarlas en operaciones de Internet, un medio esencialmente inseguro, resultaría extremadamente poco práctico, pues, el intercambio de las propias llaves no puede realizarse a través de la red.

En lo que respecta a sistemas que utilizan una combinación de llaves públicas y privadas, estos requieren que emisor y receptor utilicen algún servicio ofrecido por un tercero, el que será el guardián de las llaves públicas. Estos sistemas ofrecen mayor facilidad para uso práctico y, en materia de seguridad, son lo suficientemente aceptables como para conducir operaciones de comercio electrónico, a continuación, revisaremos con más detalle estas formas de cifrado y su uso en las firmas y certificados digitales.

Claves Simétricas

Los métodos de cifrado simétrico son aquellos que usan la misma clave para cifrar y descifrar un documento. El problema de la seguridad de las claves es el intercambio de claves entre el emisor y el receptor, ya que ambos deben utilizar la misma clave. Por lo tanto, también se debe buscar un canal de comunicación seguro para el intercambio de claves, es importante que dichas claves sean difíciles de adivinar, hoy en día ya se utilizan claves de 128 bits, lo que aumenta el "espectro" de claves posibles (2 a 128), e incluso si todas las computadoras existentes actualmente estuvieran conectadas, no se adivinaría después de miles de millones de años.

Claves Asimétricas

También se conocen como criptosistemas de clave pública. Este sistema de cifrado usa 2 claves diferentes. Uno de ellos es la clave pública (publicada por la autoridad certificadora en una carpeta específica llamada web store, que también aparece en

el certificado digital que se envía automáticamente a los destinatarios con cada mensaje), que se puede enviar a cualquier persona, y el otro es la clave privada, que debe almacenarse de forma que nadie pueda acceder a ella.

Para enviar un mensaje, la remitente cifra el mensaje utilizando la clave pública del destinatario. Una vez cifrado, solo puede ser descifrado por la clave privada del destinatario, incluso el que cifró el mensaje no puede volver a descifrarlo. Por ello, la clave pública queda perfectamente expuesta para que cualquiera que quiera comunicarse con el destinatario pueda hacerlo, el par de claves se genera durante el proceso de inicio de sesión (al recibir un certificado digital) y el propio navegador la utiliza para llamar a la generada una para el algoritmo RSA.

En las computadoras modernas, es fácil multiplicar dos números grandes para obtener un número compuesto, pero lo contrario es muy difícil, dado el número compuesto, restarlo para encontrar cada uno de esos dos números. Aunque 128 bits se consideran suficientes para las claves de cifrado simétrico, dado el progreso de la tecnología moderna, en este caso se recomienda que la clave pública sea de al menos 1024 bits.

Firmas digitales

La firma digital es la transformación de un mensaje en un texto incomprensible, mediante la utilización del cifrado asimétrico. Resulta tan efectiva en su función de dar seguridad al mensaje porque al ser aplicada se fusiona con este, además es distinta para cada mensaje que se aplica. Una típica transacción con firma digital comienza cuando el firmante está de acuerdo con el contenido del documento que desea firmar.

Luego un software específico crea una imagen digital o resumen del mensaje mediante la aplicación de una función denominada Hash Function. El resultado de la aplicación de esta función se lo conoce como Hash Result y consiste en un código único del mensaje. De esta forma si el mensaje es modificado, el Hash Result será diferente. Por último, el software encripta el Hash Result con la firma digital mediante la aplicación de la clave privada del firmante. La verificación de la firma digital se realiza calculando una nueva función Hash Result del mensaje original

utilizando la misma función Hash Function que se utilizó para crear la firma digital. Finalmente, utilizando la clave pública del certificado del firmante, el destinatario verifica que la firma digital proviene de la clave privada del firmante y que el nuevo Hash Result es el mismo que el de la firma digital.

La firma obtenida es única tanto para el mensaje como para la clave privada que se utilizó para su creación. El receptor realiza esta operación comunicándose con el registro de claves públicas donde se encuentra registrado el certificado correspondiente. Además del emisor y el receptor, para que el sistema funcione se requiere de terceras partes confiables, estas son las Autoridades de Certificación.

Para obtener una firma digital, la persona interesada, luego de crear las claves debe presentarse ante la autoridad certificadora para registrar su clave pública, acreditando su identidad y/o cualquier otra circunstancia requerida para obtener el certificado que le permita firmar el documento tratado. La información es almacenada en Registros a los cuales se puede acceder on line para saber la validez, vigencia o cualquier otra situación relacionada con los certificados

Certificados digitales

Uno de los problemas que se presentan en Internet es la identificación de personas o entidades, por ejemplo, cómo asegurar que una clave pública encontrada en Internet realmente pertenece a la persona a la que dice pertenecer, una posible solución es el uso de un certificado digital, que es un archivo digital intransferible ni modificable emitido por una autoridad de certificación de terceros de confianza que vincula claves públicas a personas o entidades.

Tipos de Certificados Digitales

Hay dos tipos principales de certificados digitales que son importantes para la construcción de un sitio Web seguro y éstos son:

Certificados del servidor: Los certificados del servidor permiten simplemente que los visitantes del sitio Web transfieran con seguridad su información personal como la información de las tarjetas de crédito y de la cuenta bancaria sin la preocupación de hurto. Los certificados del servidor son también responsables de validar la identidad de los dueños del sitio Web de modo que los visitantes puedan sentirse

como si estuvieran ocupando una fuente legítima cuando crean o ingresan contraseñas.

Certificados personales: Los certificados personales permiten validar la identidad de los visitantes del sitio Web e incluso restringir su acceso a ciertas porciones del mismo. Los certificados personales se pueden utilizar para cosas tales como enviar y recibir e-mail para la información privada de la cuenta como contraseñas olvidadas o la información del nombre de usuario. Los certificados personales son ideales para las comunicaciones tales como abastecimiento de socios y surtidores controlados, que tienen acceso al sitio para las fechas de envío, disponibilidad del producto, e incluso la gerencia de inventario.

La mayor parte de los protocolos estándares que son adoptados extensamente para las comunicaciones electrónicas confían en los siguientes certificados digitales:

El SSL: Se acepta extensamente como el estándar básico para la autentificación del Web browser y del servidor, e intercambio de datos seguro en Internet, y son el tipo más común de seguridad. Tanto para servidor como para cliente.

S/MIME: protocolo multipropósito seguro de las extensiones del correo del Internet, se considera como el estándar básico para e-mail seguro y EDI (intercambio de los datos electrónicos).

Certificados de firma de objetos: se usan para identificar al autor de ficheros o porciones de código en cualquier lenguaje de programación que se deba ejecutar en red.

Certificado para AC: para identificar a las propias Autoridades Certificadoras. Es usado por el software cliente para certificar la confianza o no de un certificado.

Niveles de Certificados

Clase 1: emitidos y comunicados electrónicamente a personas físicas, y relaciona el nombre de usuario o su alias y su dirección de e-mail con el registro llevado por el AC. No autentican la identidad del usuario. Son usados fundamentalmente para e- mail y Web Browsing, afianzando la seguridad de sus entornos. En general no se usa en ambientes comerciales.

Clase 2: son emitidos a personas físicas, y confirman la veracidad de la información aportada en el acto de presentar la aplicación que no difiere de la que surge de alguna base de datos de usuarios reconocidos. Es usado para comunicaciones intra-inter organizaciones vía e-mail; transacciones comerciales de bajo riesgo; validación de software y suscripciones on line.

Clase 3: emitidos a personas físicas, para asegurar la identidad del suscriptor, y a organizaciones públicas y privadas, para asegurar la existencia y nombre mediante el cotejo de los registros denunciados con los contenidos en bases de datos independientes.

Responsabilidad en los Certificados Digitales

El titular del certificado es responsable de notificar el cambio de los datos de autenticación, los mismos u otros posibles eventos que sólo él conoce.

La autoridad de registro es responsable de la identificación consistente y completa, realizando procedimientos confiables, ejecución correcta y confiable de las tareas de revocación, modificación y actualización, y es directamente responsable de los datos autenticados.

La autoridad de certificación es responsable de emitir pares pública y privada de dos claves que forman el eje del certificado, por otros medios o de forma segura e irrepetible, técnicamente cualitativa y de forma segura e irrepetible. No solo protege sus claves privadas, sino que también garantiza la calidad técnica de los sistemas informáticos y el acceso fácil y gratuito a listas y bibliotecas de claves públicas para verificar las firmas que emiten.

Principales usos de los Certificados Digitales

- Los Bancos pueden entregar Certificados Digitales a sus clientes, tanto individuales como corporativos, para operar a través de Home Banking o Cash Management, reemplazando el esquema de user id y password basado en claves simétricas.
- Las Grandes Empresas pueden proveer a su personal Certificados Digitales como esquema de seguridad interna para ingresar a la intranet.

- Los Supermercados pueden brindar Certificados Digitales a sus cientos de proveedores para realizar pedidos y licitaciones en línea de forma segura a través de una extranet.
- Los Organismos Públicos pueden recibir declaraciones juradas o iniciar trámites vía Internet en base a solicitudes firmadas digitalmente por sus usuarios con Certificados Digitales.

2.3.9.1. Certificados SET.

Según Molina (2007) SET proporciona los mecanismos necesarios para que tanto consumidores como comerciantes se autentifiquen mutuamente antes de que la transacción tenga lugar, simulando que el cliente se encuentra físicamente delante del mostrador del vendedor a la hora de pagar la compra, utilizando certificados digitales, los mismos que sirven como documentos de identidad digitales que permiten verificar la identidad de una persona a través de una red de telecomunicaciones, similar a la firma en las tarjetas de crédito que atestigua que el signatario es el legítimo titular. Por su parte, los certificados emitidos a comerciantes equivalen a las etiquetas mostradas en los locales, en las que se informa de que Banco se acepta las tarjetas, además de dar fe de su identidad.

El certificado es emitido y administrado por el mismo banco o emisor de la tarjeta que recibe la tarjeta de pago. Cada otra tarjeta de crédito requiere un certificado por separado. Los certificados SET son emitidos por autoridades de certificación (AC) en la jerarquía de certificados SET. Esta jerarquía asegura la autentificación válida de los participantes. También garantiza la seguridad de los datos intercambiados entre titulares, comerciantes, bancos y pasarelas de pago.

La autoridad raíz autentifica y emite certificados a las casas de medios de pago, cada una de las cuales se establece a su vez como autoridad de certificación para su marca y establece su pasarela de pagos como una AC, pudiendo así emitir certificados digitales para bancos adquirientes o procesadores de pago de terceras partes que actúan en representación de entidades adquirientes, de manera que estas puedan aceptar transacciones por Internet y convertirlas en mensajes que las redes privadas de pago pueden entender para procesar el pago.

La AC de la marca de la tarjeta autentica y emite certificados a sus bancos miembros y oficinas de crédito, que son sus autoridades de certificación establecidas. Las entidades adquirientes se transforman en AC de comerciantes, mientras que las entidades emisoras lo hacen en AC de titulares. Una vez transformada en AC de titular y/o comerciante, la entidad financiera puede autenticar y emitir certificados a sus clientes, sean estos particulares y/o comerciantes. De un modo general podría resumirse de la siguiente forma:

- Se consigue que la autentificación se extienda a todas las figuras implicadas en la transacción, pudiendo así verificar su identidad mutuamente.
- El grado de confidencialidad es mucho mayor pues la información está fuertemente cifrada para evitar fraudes.
- La integridad verifica que la información intercambiada no puede ser alterada intencionalmente, detecta incluso el cambio de un solo bit de información.
- Intimidad, con lo que las partes implicadas en la transacción sólo tendrán acceso a aquellas partes que les implique, manteniendo el resto oculto.
- La verificación inmediata de la disponibilidad del crédito e identidad del cliente al comerciante, antes de completarse la compra.
- Resolución de disputas con facilidad al ir asociadas las identidades de las partes.

Pero este sistema necesita de una serie de elementos:

- Un software de cartera del titular, programa que permite a los compradores almacenar y distribuir digitalmente sus órdenes de compra y medios de pago.
- Un software de punto de venta, programa TPV compatible con SET que acepte pedidos además de distribuir órdenes de pago en el circuito.
- Un software de pasarela de pagos que procese automáticamente los pagos, reciba peticiones de autorización/liquidación y los encamine a los sistemas tradicionales.
- Certificados. Todas las partes necesitan contar con los certificados electrónicos que garanticen la identidad de los participantes.

Certificados SET de Titular (Cardholder)

Los certificados del titular de la tarjeta actúan como una representación electrónica de la tarjeta de crédito. Sólo pueden ser emitidos a propuesta de entidades financieras, por lo que no pueden ser modificados por terceros. En el certificado, los datos relacionados con el número de tarjeta y el período de validez están encriptados con un algoritmo y no se pueden deducir mirando el certificado. El titular proporciona información a la pasarela de pago que verifica el certificado. Al solicitar un certificado, el propietario indica que planea iniciar un negocio de comercio electrónico.

El certificado se envía a la tienda junto con la orden de compra y las instrucciones de pago encriptadas. Al recibir la confirmación del propietario, la empresa puede al menos estar segura de que el banco emisor de la tarjeta ha verificado el número de la tarjeta. Los tarjetahabientes pueden solicitar tantas credenciales como tarjetas de crédito/débito existan, cada una asociada a la respectiva tarjeta. El software que utilizan los propietarios para almacenar certificados y comunicarse con los comerciantes se denomina monedero virtual o monedero electrónico.

El software se integra a los navegadores de Internet que utilizan los tarjetahabientes y también permite guardar información sobre las transacciones realizadas a lo largo del tiempo. El software es proporcionado por instituciones financieras.

Certificados SET de Comercio (Merchant)

Estos certificados reemplazan la etiqueta de la tarjeta de crédito que se muestra en los escaparates de las tiendas. Estos logotipos indican que la empresa está afiliada a una institución financiera que acepta pagos con tarjeta de crédito. Estos certificados son visados por el banco receptor y aseguran que existe un contrato válido entre las partes. Los comerciantes deben presentar un certificado por cada marca de tarjeta aceptada.

Los comerciantes deben instalar software de administración o software comercial en sus servidores para realizar transacciones comerciales en una red abierta y son compatibles con cualquier red de procesamiento de pagos que admita la especificación SET, independientemente del proveedor de servicios. El software

gestionará automáticamente el certificado de comerciante y todo el cifrado, direccionamiento, descifrado, gestión de claves públicas y privadas y comunicación con las pasarelas de pago. El software necesario lo proporciona el propio banco.

Certificados SET de Pasarela de Pagos (Payment Gateway)

Los certificados de pasarela de pago se emiten a los beneficiarios y sus procesadores de transacciones (operadores de medios de pago) y se aplican a los sistemas que manejan la autorización y recepción de mensajes. Estos certificados residen en la infraestructura de la pasarela de pago y validan los certificados de propietario y comerciante recibidos.

Cuando la pasarela confirma la operación, devuelve la autorización al comercio. La validez y seguridad de los certificados SET residen en la jerarquía de confianza que los respalda. Cada certificado está asociado a una entidad que lo firma digitalmente. Al rastrear el árbol de confianza hasta un tercero de confianza conocido (TTP), puede asegurarse de que el certificado sea válido. Por ejemplo, un certificado del titular de la tarjeta está vinculado a un certificado del emisor, que a su vez está vinculado a la marca propietaria de la tarjeta del titular de la tarjeta.

La clave raíz pública o de activación es conocida por todo el software SET y se puede utilizar para verificar todos los certificados que contiene. Las claves raíz se distribuyen mediante certificados autofirmados. Esta clave está incluida en el software distribuido por el proveedor de software SET y se comprueba si es una clave raíz válida consultando a la autoridad de certificación.

2.3.9.2. Certificado PCI DSS (Payment Card Industry – Data Security Standards).

Según Araujo (2021) es un estándar global de protección de datos para la industria que procesa pagos con tarjeta de crédito o débito. El objetivo es garantizar que todos los negocios tengan un nivel básico mínimo de seguridad que proteja los datos del titular de la tarjeta. Como muchos otros sistemas de cumplimiento, PCI DSS se actualiza de vez en cuando. Si bien la última versión es la 3.2.1, se entiende que la versión 4.0 estará disponible en el primer trimestre de 2022.

El estándar PCI DSS proporciona un conjunto de pautas y mejores prácticas para todos los aspectos de la seguridad física, lógica y administrativa. Esto incluye controles, políticas, procesos, arquitectura de red, seguridad y desarrollo de software, entre otros.

Cumplimiento de estándar PCI DSS

Si su modelo de negocio almacena, procesa o transmite datos de titulares de tarjetas, debe cumplir con PCI DSS. No importa el tamaño de la empresa. Si su empresa no procesa ni almacena los detalles de la tarjeta, pero utiliza una pasarela de pago, lo más probable es que deba cumplir con este estándar. Dado que los requisitos pueden ser menos estrictos, debe obtener la certificación de la misma manera. Por otro lado, PCI DSS establece diferentes requisitos según el número de transacciones anuales de la empresa. Es decir, los agrupa de acuerdo a lo siguiente:

- Nivel 1: Más de seis millones de transacciones por año.
- Nivel 2: De uno a seis millones de transacciones por año.
- Nivel 3: 20.000 a 1 millón de transacciones por año.
- Nivel 4: menos de 20.000 transacciones al año.

Por lo general, para los niveles 2, 3 y 4, deberá completar un cuestionario de autoevaluación conocido como SAQ o Cuestionario de autoevaluación, una herramienta de evaluación diseñada para ayudar a las empresas a evaluar el cumplimiento de PCI DSS. Para el Nivel 1, además de completar este cuestionario de autoevaluación, requieren una prueba más completa de cada requisito, ya que generalmente se trata de grandes empresas, como procesadores de pago, bancos, propietarios de botones de pago de fintech, etc.

Requisitos de PCI DSS

En total, el estándar PCI DSS tiene 12 requisitos, que se describen en 6 grupos o "metas" de cumplimiento. Para que te hagas una idea, estos requisitos vuelven a tener en cuenta más de 300 controles de seguridad.

Tabla 4

Metas y requisitos de PCI DSS

Metas	Requisitos
	1. Instale y mantenga configuraciones de firewall para proteger los datos del titular de la tarjeta.
1. Crear y mantener sistemas y redes seguras	2. No utilice valores predeterminados proporcionados por el proveedor para las contraseñas del sistema y otros parámetros de seguridad.
2. Proteja los datos del titular de la tarjeta	3. Proteja los datos almacenados del titular de la tarjeta. 4. Cifre la transmisión de datos del titular de la tarjeta en redes públicas abiertas.
3. Mantener un programa de administración de vulnerabilidades	5. Proteja todos los sistemas contra malware y actualice regularmente los programas o software antivirus. 6. Desarrollar y mantener sistemas y aplicaciones seguros.
4. Incrementar medidas sólidas de control de acceso	7. Restrinja el acceso a los datos del titular de la tarjeta en función de la necesidad empresarial de conocerlos. 8. Identificar y verificar el acceso a los componentes del sistema. 9. Limite el acceso físico a los datos del titular de la tarjeta

5. Supervisar y evaluar las redes con regularidad	10. Rastree y supervise todos los accesos a los recursos de red y a los datos del titular de tarjeta. 11. Probar periódicamente los sistemas y procesos de seguridad.
6. Mantener una política de seguridad de la información	12. Mantener una política que aborde la seguridad de la información para todo el personal.

Nota: Esta tabla muestra las metas y requisitos del estándar PCI DSS.

La adopción de la norma PCI permite a los comercios contar con los siguientes beneficios:

- Promover la integridad del comercio y aumentar la confianza de los consumidores en el negocio.
- Incrementar las ventas como consecuencia del aumento en la confianza de los consumidores.
- Proteger al comercio de posibles pérdidas de ingresos, investigaciones no deseadas y costos legales.
- Reducir el riesgo de atención no deseada de la prensa como resultado de un compromiso fuga de información de clientes.
- Proyectar mayor conciencia de los controles y medidas preventivas de seguridad disponibles para el comercio.
- Reducir las disputas de Tarjetahabientes y costos asociados a transacciones fraudulentas resultantes de un compromiso de información.
- Prevenir el robo masivo de información de clientes.
- Facilitar la adopción de estándares de seguridad válidos a nivel global.
- Generar una herramienta que establece las posibles vulnerabilidades que tiene el sistema de información.

2.3.9.3. Certificación Visa.

Según Visa (2022) menciona que la insignia de Visa Secure en los sitios web de comerciantes participantes cuando compra en línea, sus compras en línea están protegidas cuando paga con Visa. Visa ha desarrollado un programa para ayudarlo a verificar su identidad cuando compra en línea en los sitios comerciales participantes. Somos un líder global confiable en redes y pagos digitales, con la misión de eliminar barreras y atraer a más personas a la economía global. Porque creemos que una economía inclusiva y ubicua empodera a todos, en todas partes.

Beneficios

- Visa protege los datos al momento de la compra e informa al banco sobre cada transacción.
- Toda la tecnología verifica los datos para garantizar la seguridad de las transacciones.
- Todas las compras son monitoreadas 24/7, sin importar el monto.
- Puede comprar desde su teléfono, dispositivo móvil o computadora en cualquier tienda del mundo.
- Seguro sin tocar nada.

2.3.9.4. Certificación MasterCard.

Según Applus Laboratories (2022) todas las soluciones de pago de Mastercard deben cumplir con la Evaluación de Cumplimiento y Verificación de Seguridad (CAST) de Mastercard. El programa CAST evalúa la conformidad de las aplicaciones implementadas en tarjetas (con y sin contacto) y chips de seguridad de pagos móviles con los requisitos de seguridad. Para cumplir con las especificaciones de Mastercard, las aplicaciones de pago deben funcionar con un chip (IC) precertificado por EMVCo.

Beneficios

- One stop shop para la certificación integral para la seguridad de su aplicación de pago frente a los requisitos de Mastercard y otros esquemas de pago, incluidas las pruebas de EMVCo y GlobalPlatform.

- Acelerar el procedimiento de certificación.

2.3.9.5. Certificación American Express.

Applus Laboratories (2022) indica que las soluciones de pago basadas en el programa American Express deben pasar por el proceso de aprobación de American Express. Este proceso incluye pruebas funcionales y evaluación de seguridad a realizar por un laboratorio acreditado bajo este plan de pago. AMEX tiene diferentes especificaciones de prueba según el tipo de producto. Como parte de la asociación EMVCo y GlobalPlatform, el proceso de aprobación también puede incluir el cumplimiento de las especificaciones EMV y GP.

Applus+ ofrece sus servicios de certificación de sistemas utilizando la marca de certificación global Applus+. Certificamos una variedad de estándares de acreditación globales, nacionales y específicos de la industria para ayudar a nuestros clientes a mejorar sus operaciones y demostrar a los clientes finales nuestro compromiso con la excelencia y la mejora continua.

Beneficios

- One stop shop para evaluar soluciones de pago contra American Express y otros sistemas de pago, incluidas las pruebas de EMVCo y GlobalPlatform
- Acelera el proceso de certificación para reducir el tiempo de comercialización.

2.3.9.6. Certificación Diners Club.

Según Diners Club (2022) la certificación Diners protege los datos con los más altos estándares de seguridad en la industria financiera y garantiza la integridad, confidencialidad y disponibilidad de sus programas, tecnología e información. Además, Diners utiliza medidas de seguridad diseñadas para proteger los datos personales. Además, exigimos a los empleados de Diners que procesan dichos datos personales que mantengan la confidencialidad e integridad en el procesamiento de dichos datos personales, con el máximo respeto por la privacidad de las personas.

Beneficio

- Diners destina importantes inversiones de su presupuesto anual para mantener e implementar los más altos estándares de seguridad y protección, siempre siguiendo las mejores prácticas nacionales e internacionales.

2.3.9.7. Certificación Discover.

Applus Laboratories (2022) menciona que las tarjetas que utilizan la aplicación de pago Discover deben pasar por un proceso de aprobación especial para demostrar su seguridad, funcionalidad y compatibilidad antes de ser lanzadas al mercado. Este plan de pago requiere que se realice un conjunto de pruebas requeridas por Discover en un laboratorio acreditado. Además, Discover requiere que su aplicación de pago (D-PAS) se implemente en un chip precertificado (IC) EMVCo (seguro). Discover ha sido acreditado por Applus Laboratories para realizar pruebas funcionales y evaluaciones de seguridad según sus especificaciones. También somos un laboratorio acreditado por EMVCo y acreditado por GlobaPlatform, lo que nos permite realizar todas las pruebas requeridas en el proceso de aprobación de Discover.

Beneficios

- One stop shop para la certificación integral de la seguridad y la funcionalidad de su solución de pago según lo exigen Discover y otras soluciones de pago, incluidas las pruebas de EMVCo y GlobalPlatform.
- Acelerar el procedimiento de certificación.

2.3.9.8. Certificación Alia.

Según Banco Solidario (2018) el certificado Alia por The Smart Campaign para cumplir con los estándares internacionales de protección al cliente. La certificación fue aprobada durante la revisión inicial en septiembre de 2021.

Beneficio

- Gestionar el desempeño social, la protección del cliente y la calidad de los productos y servicios.

2.3.9.9. Certificación UnionPay.

Según UnionPay (2020) de acuerdo con el Reglamento Operativo Internacional de UnionPay, para ser un proveedor de tarjetas UnionPay, una empresa debe aprobar la certificación UnionPay, cuyo objetivo es garantizar que la fabricación de la tarjeta UnionPay cumpla estrictamente con las especificaciones técnicas unificadas, para proteger la seguridad de las cuentas y transacciones de UnionPay, y para garantizar la interoperabilidad, seguridad y estabilidad de los productos de tarjetas UnionPay.

Beneficios

- Garantizar que los productos de la tarjeta UnionPay implementen estrictamente los estándares técnicos unificados de UnionPay.
- Protejer la información de la cuenta de la tarjeta UnionPay y la seguridad de las transacciones.
- Asegurar la universalidad, seguridad y estabilidad de los productos de la tarjeta UnionPay.

2.4. Legal

2.4.1. Constitución de la Republica del ecuador

Según la Constitución de la República del Ecuador (2015) Registro Oficial 449 de 20-oct.-2008 establece lo siguiente:

Artículo 15.- El derecho a desarrollar actividades económicas, en forma individual o colectiva, conforme a los principios de solidaridad, responsabilidad social y ambiental.

Artículo 19.- El derecho a la protección de datos de carácter personal, que incluye el acceso y la decisión sobre información y datos de este carácter, así como su correspondiente protección. La recolección, archivo, procesamiento, distribución o difusión de estos datos o información requerirán la autorización del titular o el mandato de la ley.

Artículo 226.- Las instituciones del Estado, sus organismos, dependencias, las servidoras o servidores públicos y las personas que actúen en virtud de una potestad

estatal ejercerán solamente las competencias y facultades que les sean atribuidas en la Constitución y la ley. Tendrán el deber de coordinar acciones para el cumplimiento de sus fines y hacer efectivo el goce y ejercicio de los derechos reconocidos en la Constitución.

Artículo 227.- La administración pública constituye un servicio a la colectividad que se rige por los principios de eficacia, eficiencia, calidad, jerarquía, desconcentración, descentralización, coordinación, participación, planificación, transparencia y evaluación.

Artículo 303.- La formulación de las políticas monetaria, crediticia, cambiaria y financiera es facultad exclusiva de la Función Ejecutiva y se instrumentará a través del Banco Central. La ley regulará la circulación de la moneda con poder liberatorio en el territorio ecuatoriano.

La ejecución de la política crediticia y financiera también se ejercerá a través de la banca pública.

El Banco Central es una persona jurídica de derecho público, cuya organización y funcionamiento será establecido por la ley.

2.4.2. Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos

Según el Congreso Nacional (2022) con Registro Oficial Suplemento 557 se aprobó en Ecuador la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos que establece lo siguiente:

Que es indispensable que el Estado Ecuatoriano cuente con herramientas jurídicas que le permitan el uso de los servicios electrónicos, incluido el comercio electrónico y acceder con mayor facilidad a la cada vez más compleja red de los negocios internacionales; y, En uso de sus atribuciones, expide la siguiente:

Artículo 1.- Objeto de la Ley. - Esta Ley regula los mensajes de datos, la firma electrónica, los servicios de certificación, la contratación electrónica y telemática, la prestación de servicios electrónicos, a través de redes de información, incluido el comercio electrónico y la protección a los usuarios de estos sistemas.

Artículo 5.- Confidencialidad y reserva. - Se establecen los principios de confidencialidad y reserva para los mensajes de datos, cualquiera sea su forma,

medio o intención. Toda violación a estos principios, principalmente aquellas referidas a la intrusión electrónica, transferencia ilegal de mensajes de datos o violación del secreto profesional, será sancionada conforme a lo dispuesto en esta Ley y demás normas que rigen la materia.

Artículo 9.- Protección de datos. - Para la elaboración, transferencia o utilización de bases de datos, obtenidas directa o indirectamente del uso o transmisión de mensajes de datos, se requerirá el consentimiento expreso del titular de éstos, quien podrá seleccionar la información a compartirse con terceros.

La recopilación y uso de datos personales responderá a los derechos de privacidad, intimidad y confidencialidad garantizados por la Constitución Política de la República y esta ley, los cuales podrán ser utilizados o transferidos únicamente con autorización del titular u orden de autoridad competente.

No será preciso el consentimiento para recopilar datos personales de fuentes accesibles al público, cuando se recojan para el ejercicio de las funciones propias de la administración pública, en el ámbito de su competencia, y cuando se refieran a personas vinculadas por una relación de negocios, laboral, administrativa o contractual y sean necesarios para el mantenimiento de las relaciones o para el cumplimiento del contrato.

El consentimiento a que se refiere este artículo podrá ser revocado a criterio del titular de los datos; la revocatoria no tendrá en ningún caso efecto retroactivo

Artículo 12.- Duplicación del mensaje de datos. - Cada mensaje de datos será considerado diferente. En caso de duda, las partes pedirán la confirmación del nuevo mensaje y tendrán la obligación de verificar técnicamente la autenticidad del mismo.

De las firmas electrónicas, certificados de firma electrónica, entidades de certificación de información, organismos de promoción de los servicios electrónicos, y de regulación y control de las entidades de certificación acreditadas.

Artículo 13.- Firma electrónica. - Son los datos en forma electrónica consignados en un mensaje de datos, adjuntados o lógicamente asociados al mismo, y que puedan ser utilizados para identificar al titular de la firma en relación con el mensaje

de datos, e indicar que el titular de la firma aprueba y reconoce la información contenida en el mensaje de datos.

Artículo 16.- La firma electrónica en un mensaje de datos. - Cuando se fijare la firma electrónica en un mensaje de datos, aquélla deberá enviarse en un mismo acto como parte integrante del mensaje de datos o lógicamente asociada a éste. Se presumirá legalmente que el mensaje de datos firmado electrónicamente conlleva la voluntad del emisor, quien se someterá al cumplimiento de las obligaciones contenidas en dicho mensaje de datos, de acuerdo a lo determinado en la Ley.

Artículo 18.- Duración de la firma electrónica. - Las firmas electrónicas tendrán duración indefinida. Podrán ser revocadas, anuladas o suspendidas de conformidad con lo que el reglamento a esta ley señale.

Artículo 19.- Extinción de la firma electrónica. - La firma electrónica se extinguirá por:

a) Voluntad de su titular;
b) Fallecimiento o incapacidad de su titular;
c) Disolución o liquidación de la persona jurídica, titular de la firma; y,
d) Por causa judicialmente declarada.

La extinción de la firma electrónica no exime a su titular de las obligaciones previamente contraídas derivadas de su uso.

De las entidades de certificación de información

Artículo 29.- Entidades de certificación de información. - Son las empresas unipersonales o personas jurídicas que emiten certificados de firma electrónica y pueden prestar otros servicios relacionados con la firma electrónica, autorizadas por el Consejo Nacional de Telecomunicaciones, según lo dispuesto en esta ley y el reglamento que deberá expedir el presidente de la República.

Artículo 31.- Responsabilidades de las entidades de certificación de información acreditadas. – Las entidades de certificación de información serán responsables hasta de culpa leve y responderán por los daños y perjuicios que causen a cualquier persona natural o jurídica, en el ejercicio de su actividad, cuando incumplan las obligaciones que les impone esta Ley o actúen con negligencia, sin perjuicio de las sanciones previstas en la Ley Orgánica de Defensa del Consumidor. Serán también

responsables por el uso indebido del certificado de firma electrónica acreditado, cuando éstas no hayan consignado en dichos certificados, de forma clara, el límite de su uso y del importe de las transacciones válidas que pueda realizar. Para la aplicación de este artículo, la carga de la prueba le corresponderá a la entidad de certificación de información.

Los contratos con los usuarios deberán incluir una cláusula de responsabilidad que reproduzca lo que señala el primer inciso. Cuando la garantía constituida por las entidades de certificación de información acreditadas no cubra las indemnizaciones por daños y perjuicios, aquellas responderán con su patrimonio.

Artículo 32.- Protección de datos por parte de las entidades de certificación de información acreditadas. - Las entidades de certificación de información garantizarán la protección de los datos personales obtenidos en función de sus actividades, de conformidad con lo establecido en el artículo 9 de esta ley.

Artículo 33.- Prestación de servicios de certificación por parte de terceros. - Los servicios de certificación de información podrán ser proporcionados y administrados en todo o en parte por terceros. Para efectuar la prestación, éstos deberán demostrar su vinculación con la Entidad de Certificación de Información.

El Consejo Nacional de Telecomunicaciones, establecerá los términos bajo los cuales las Entidades de Certificación de Información podrán prestar sus servicios por medio de terceros.

De los derechos de los usuarios o consumidores de servicios electrónicos

Artículo 49.- Consentimiento para el uso de medios electrónicos. - De requerirse que la información relativa a un servicio electrónico, incluido el comercio electrónico, deba constar por escrito, el uso de medios electrónicos para proporcionar o permitir el acceso a esa información, será válido si:

a) El consumidor ha consentido expresamente en tal uso y no ha objetado tal consentimiento; y,

b) El consumidor en forma previa a su consentimiento ha sido informado, a satisfacción, de forma clara y precisa, sobre:

1. Su derecho u opción de recibir la información en papel o por medios no electrónicos;

2. Su derecho a objetar su consentimiento en lo posterior y las consecuencias de cualquier tipo al hacerlo, incluidas la terminación contractual o el pago de cualquier tarifa por dicha acción;
3. Los procedimientos a seguir por parte del consumidor para retirar su consentimiento y para actualizar la información proporcionada; y,
4. Los procedimientos para que, posteriormente al consentimiento, el consumidor pueda obtener una copia impresa en papel de los registros electrónicos y el costo de esta copia, en caso de existir.

De las infracciones informáticas

Artículo 57.- Infracciones informáticas. - Se considerarán infracciones informáticas, las de carácter administrativo y las que se tipifican, mediante reformas al Código Penal, en la presente ley.

Reformas al código penal

Artículo 58.- A continuación del Art. 202, inclúyase los siguientes artículos enumerados:
"Artículo ....- El que empleando cualquier medio electrónico, informático o afín, violentare claves o sistemas de seguridad, para acceder u obtener información protegida, contenida en sistemas de información; para vulnerar el secreto, confidencialidad y reserva, o simplemente vulnerar la seguridad, será reprimido con prisión de seis meses a un año y multa de quinientos a mil dólares de los Estados Unidos de Norteamérica.
Si la información obtenida se refiere a seguridad nacional, o a secretos comerciales o industriales, la pena será de uno a tres años de prisión y multa de mil a mil quinientos dólares de los Estados Unidos de Norteamérica. La divulgación o la utilización fraudulenta de la información protegida, así como de los secretos comerciales o industriales, será sancionada con pena de reclusión menor ordinaria de tres a seis años y multa de dos mil a diez mil dólares de los Estados Unidos de Norteamérica. Si la divulgación o la utilización fraudulenta se realiza por parte de la persona o personas encargadas de la custodia o utilización legítima de la

información, éstas serán sancionadas con pena de reclusión menor de seis a nueve años y multa de dos mil a diez mil dólares de los Estados Unidos de Norteamérica.
Artículo ....- Obtención y utilización no autorizada de información.- La persona o personas que obtuvieren información sobre datos personales para después cederla, publicarla, utilizarla o transferirla a cualquier título, sin la autorización de su titular o titulares, serán sancionadas con pena de prisión de dos meses a dos años y multa de mil a dos mil dólares de los Estados Unidos de Norteamérica."
"Artículo ....- Falsificación electrónica.- Son reos de falsificación electrónica la persona o personas que con ánimo de lucro o bien para causar un perjuicio a un tercero, utilizando cualquier medio, alteren o modifiquen mensajes de datos, o la información incluida en éstos, que se encuentre contenida en cualquier soporte material, sistema de información o telemático, ya sea:

1. Alterando un mensaje de datos en alguno de sus elementos o requisitos de carácter formal o esencial;
2. Simulando un mensaje de datos en todo o en parte, de manera que induzca a error sobre su autenticidad;
3. Suponiendo en un acto la intervención de personas que no la han tenido o atribuyendo a las que han intervenido en el acto, declaraciones o manifestaciones diferentes de las que hubieren hecho.

El delito de falsificación electrónica será sancionado de acuerdo a lo dispuesto en este capítulo.".
Artículo 61.- A continuación del Art. 415 del Código Penal, inclúyanse los siguientes artículos enumerados.
"Artículo ....- Daños informáticos.- El que dolosamente, de cualquier modo o utilizando cualquier método, destruya, altere, inutilice, suprima o dañe, de forma temporal o definitiva, los programas, datos, bases de datos, información o cualquier mensaje de datos contenido en un sistema de información o red electrónica, será reprimido con prisión de seis meses a tres años y multa de sesenta a ciento cincuenta dólares de los Estados Unidos de Norteamérica.
La pena de prisión será de tres a cinco años y multa de doscientos a seis cientos dólares de los Estados Unidos de Norteamérica, cuando se trate de programas, datos, bases de datos, información o cualquier mensaje de datos contenido en un

sistema de información o red electrónica, destinada a prestar un servicio público o vinculada con la defensa nacional.

"Artículo ....- Apropiación ilícita.- Serán reprimidos con prisión de seis meses a cinco años y multa de quinientos a mil dólares de los Estados Unidos de Norteamérica, los que utilizaren fraudulentamente sistemas de información o redes electrónicas, para facilitar la apropiación de un bien ajeno, o los que procuren la transferencia no consentida de bienes, valores o derechos de una persona, en perjuicio de ésta o de un tercero, en beneficio suyo o de otra persona alterando, manipulando o modificando el funcionamiento de redes electrónicas, programas informáticos, sistemas informáticos, telemáticos o mensajes de datos.

Artículo ....- La pena de prisión de uno a cinco años y multa de mil a dos mil dólares de los Estados Unidos de Norteamérica, si el delito se hubiere cometido empleando los siguientes medios

1. Inutilización de sistemas de alarma o guarda;
2. Descubrimiento descifrado de claves secretas o encriptadas;
3. Utilización de tarjetas magnéticas o perforadas;
4. Utilización de controles o instrumentos de apertura a distancia; y,
5. Violación de seguridades electrónicas, informáticas u otras semejantes.".

2.4.3. Código Orgánico Integral Penal

Según el Congreso Nacional (2014) con Registro Oficial Suplemento 180 se aprobó en Ecuador el Código orgánico integral penal (COIP), que establece lo siguiente:

Artículo 186.- Estafa. – La persona que, para obtener un beneficio patrimonial para sí misma o para una tercera persona, mediante la simulación de hechos falsos o la deformación u ocultamiento de hechos verdaderos, induzca a error a otra, con el fin de que realice un acto que perjudique su patrimonio o el de una tercera, será sancionada con pena privativa de libertad de cinco a siete años. La pena máxima se aplicará a la persona que:

1. Defraude mediante el uso de tarjeta de crédito, débito, pago o similares, cuando ella sea alterada, clonada, duplicada, hurtada, robada u obtenida sin legítimo consentimiento de su propietario.

2. Defraude mediante el uso de dispositivos electrónicos que alteren, modifiquen, clonen o dupliquen los dispositivos originales de un cajero automático para capturar, almacenar, copias o reproducir información de tarjetas de crédito, débito, pago o similares.
3. Entregue certificación falsa sobre las operaciones o inversiones que realice la persona jurídica.
4. Induzca a la compra o venta pública de valores por medio de cualquier acto, práctica, mecanismo o artificio engañoso o fraudulento.
5. Efectúe cotizaciones o transacciones ficticias respecto de cualquier valor.

2.4.4. Norma para la autorización, vigilancia y supervisión de las administradoras de los sistemas auxiliares de pago

Según el Banco Central del Ecuador (2022) en la Resolución Administrativa Nro. BCE-GG-007-2022 establece lo siguiente:

Alcance y definiciones

Artículo 1.- Sistemas auxiliares de pago. - Conjunto de políticas, normas, instrumentos, procedimientos y servicios articulados y coordinados, públicos o privados, establecidos para efectuar transferencias de recursos, remesas de dinero o compensación entre sus distintos participantes.

Artículo 2.- Alcance. - La presente norma rige para todas las administradoras de los sistemas auxiliares de pago (ASAP) y los servicios que aquellas presten a las entidades financieras, en los términos establecidos en el artículo precedente. Artículo 3.- Servicio. - Los servicios que pueden prestar las ASAP se encuentran detallados en las disposiciones emitidas por la Junta de Política y Regulación Monetaria.

De la autorización

Artículo 4.- Para ser autorizadas como ASAP, las entidades deberán solicitarlo, por escrito, al Banco Central del Ecuador, adjuntando la siguiente documentación:

1. Escritura pública de constitución de la compañía, conjuntamente con las últimas reformas estatutarias y la inscripción en el Registro Mercantil, que acrediten su existencia legal, las mismas que deberán incluir el estatuto social vigente; así como, la nómina de accionistas y representantes legales.

2. Certificado de haber cumplido sus obligaciones emitido por la Superintendencia de Compañías Valores y Seguros, y, Superintendencia de Bancos y/o Superintendencia de Economía Popular y Solidaria, según corresponda.

3. Detalle del servicio que requiere autorizar.

4. Detalle de los requisitos que solicita a sus clientes para operar en el servicio que requiere autorizar.

5. Listado de puntos de atención; y,

6. Esquema operativo del servicio que requiere autorizar, incluidos los procesos de compensación y conectividad al BCE, de ser el caso.

Artículo 6.- Las entidades que requieran autorización para el servicio de pasarelas de pago y agregación de pago, adicionalmente a los requisitos del artículo 4, deberán adjuntar el certificado de estándar de Seguridad de Datos para la Industria de Tarjeta de Pago PCI-DSS o estándares ISO para pagos y otros servicios financieros.

Artículo 7.- Las ASAP que, adicionalmente, requieran prestar los servicios de recaudación de recursos públicos deberán cumplir con los requisitos establecidos por el Banco Central del Ecuador para su calificación como corresponsal, antes de iniciar operaciones.

Artículo 8.- Todos los documentos remitidos por las entidades para la autorización como ASAP, detallados en los artículos precedentes, deberán observar la información contenida en el Anexo “Detalle de Requisitos para Autorización como ASAP”, para su efectivo cumplimiento.

Artículo 9.- Una vez recibida la solicitud de autorización por parte de las entidades, el Banco Central del Ecuador dentro del término de quince (15) días podrá autorizar o negar la solicitud de la entidad.

De la vigilancia y supervisión

Artículo 10.- El Banco Central del Ecuador ejercerá permanentemente la vigilancia y supervisión preventiva extra situ y visitas de inspección in situ, sin restricción alguna, a fin de evaluar la operación, gobierno, control de riesgos y requerimientos financieros. Complementariamente, se emitirán oficios de colaboración con otras entidades de control del país, de ser el caso.

Artículo 11.- Con la finalidad de realizar la vigilancia, las ASAP remitirán al Banco Central del Ecuador, hasta los diez (10) primeros días de cada mes, la estructura de información transaccional, de acuerdo a las especificaciones técnicas establecidas en el instructivo que se dicte para el efecto.

Artículo 12.- Para la supervisión, las ASAP están obligadas a:

1. Facilitar las inspecciones en las oficinas, instalaciones, equipos y sistemas de tecnologías de información y comunicación de los ASAP;

2. Remitir información en los plazos y términos señalados por el Banco Central del Ecuador;

3. Remitir planes de contingencia y continuidad, política de gestión de riesgos, política de seguridad de la información;

4. Elaborar los planes de acción con medidas correctivas dispuestos por el Banco Central del Ecuador, respecto de los mecanismos adecuados para la operación, gobierno, control de riesgos y requerimientos financieros;

5. Cumplir los términos acordados mediante contratos con sus clientes, en especial en lo relacionado a los plazos de transferencias de recursos, medios de pago relacionados con el servicio, canales utilizados y alcance del servicio; y,

6. Observar las disposiciones emitidas por la Junta de Regulación y Política Monetaria o el Banco Central del Ecuador, en lo relacionado a las ASAP.

Artículo 13.- El proceso de supervisión in situ, se iniciará notificando mediante oficio a las ASAP, en el cual se solicitará la documentación referente a la operación, gobierno, control de riesgos y requerimientos financieros.

Artículo 14.- El Banco Central del Ecuador elaborará un plan de supervisión anual de las ASAP que será aprobado por la Gerencia General, y los avances de dicho plan, se informarán de manera trimestral a esta autoridad.

Artículo 15.- El Banco Central del Ecuador, de oficio o a petición de parte, efectuará el seguimiento de personas naturales o jurídicas que, sin autorización, se encuentren brindando los servicios que pueden prestar exclusivamente las ASAP autorizadas por el Banco Central del Ecuador.

2.4.5. Junta de Política y Regulación Monetaria y Financiera

Según la Junta de Política y Regulación Monetaria y Financiera (2018) en la Resolución No. 441-2018-M establece lo siguiente:

Medios de pago electrónicos

Artículo 1.- Son medios de pago electrónicos los mecanismos electrónicos o digitales utilizados para la transferencia de recursos y/o pagos de todo tipo de obligaciones de conformidad con la autorización que le otorgue el respectivo organismo de control.

Artículo 2.- Los pagos realizados a través de medios electrónicos o digitales no podrán ser repudiados, revocados o dejados sin efecto por las entidades participantes.

Artículo 3.- Las transacciones financieras efectuadas a través de medios de pagos electrónicos serán liquidadas en el Banco Central del Ecuador.

Artículo 4.- El Banco Central del Ecuador establecerá las condiciones para la liquidación de las transacciones efectuadas con medios de pago electrónicos.

Artículo 5.- De ser el caso el Banco Central del Ecuador aplicará las sanciones de acuerdo a lo dispuesto en el COMF, y en el Reglamento o Norma aplicable.

Alcance y Definiciones

Artículo 6.- Alcance: La presente normativa rige para todos los Sistemas Auxiliares de Pago (SAP) autorizados por el Banco Central del Ecuador, para que administren plataformas de pago móvil.

Artículo 7.- Definiciones: Para efectos de esta resolución los términos señalados a continuación tendrán el siguiente significado:

l. BCE: Banco Central del Ecuador.

2. Compensación: Proceso ejecutado por los sistemas auxiliares de pagos autorizados que administran plataformas de pago móvil, para determinar la posición neta a favor o en contra, que los participantes deben pagar o recibir en sus cuentas corrientes que mantienen en el BCE.

3. COMF: Código Orgánico Monetario y Financiero.

4. JPRMF: Junta de Política y Regulación Monetaria y Financiera.

5. Pago Móvil: Son aquellas transferencias de fondos originadas desde un teléfono celular asociado a una cuenta en una entidad del sistema financiero nacional, para efectuar cobros y pagos.

6. PPM: Plataforma de Pagos Móviles la cual consiste en un conjunto de componentes de hardware, software y normas operativas que inter - operan y permiten el procesamiento de las transacciones de pago móvi1.

7. SAP: Sistemas Auxiliares de Pago: Son el conjunto de políticas, normas, instrumentos, procedimientos y servicios articulados y coordinados, públicos o privados, autorizados por el Banco Central del Ecuador, interconectados con el sistema central de pagos, establecidos para efectuar transferencias de recursos y compensación entre sus distintos participantes.

De la autorización y servicios

Artículo 8.- El BCE autorizará a las entidades que administren PPM como SAP, que estén debidamente autorizadas como servicios auxiliares del sistema financiero por la Superintendencia de Bancos o Superintendencia de Economía Popular y Solidaria para prestar este servicio.

Artículo 9.- Los sistemas auxiliares de pago podrán administrar la PPM previa autorización del BCE. La autorización se solicitará por escrito adjuntando la documentación técnica, operativa, financiera y legal que el BCE defina.

Artículo 10.- La autorización conferida a los SAP para administrar una PPM, no constituye garantía o certificación alguna por parte del BCE respecto de su capacidad legal, financiera y operativa, como tampoco representa garantía o certificación alguna sobre las operaciones de sus participantes.

Artículo 11.- Las PPM podrán brindar los servicios de:

1. Transferencias electrónicas entre cuentas de clientes de las entidades del sistema financiero nacional.

2. Depósitos y retiros, a través de las ventanillas o canales electrónicos de otras entidades financieras o de corresponsales no bancarios.

3. Pago de ¡impuestos, tasas y contribuciones.

4. Pago de consumo de servicios básicos.

5. Pago de consumo de servicios recibidos de entidades del sector público y privado.

6. Pagos y cobros por compras de bienes y/o servicios a entidades del sector público y privado.

7. Cobro del Bono de Desarrollo Humano y de otras subvenciones del Gobierno Nacional.

8. Otros servicios que determine el BCE. Los trámiles de autorización solicitados al BCE por parte de los SAP estarán sujetos a los plazos y condiciones establecidos en la normativa que para el efecto emita el BCE.

Artículo 12.- El BCE verificará acciones o prácticas restrictivas por parte de las PPM con tas instituciones del sistema financiero nacional que deseen usar sus servicios. El BCE aplicará el procedimiento sancionador correspondiente.

Tarifas por servicio

Articulo 105.- Tarifa de USD 0.35 (treinta y cinco centavos) más los impuestos de ley por concepto de recaudación de fondos públicos, que aplicarán los SAP a sus clientes.

De los sistemas auxiliares de pago

Artículo 1.- Alcance: La presente normativa rige para todas aquellas entidades catalogadas como sistemas auxiliares de pagos y sus entidades administradoras, así como, cualquier infraestructura de pagos o de transferencias de recursos monetarios que actúen en el mercado.

De la autorización

Artículo 3.- Las entidades que deseen calificarse para operar como sistemas auxiliares de pagos deberán solicitar, por escrito, la autorización previa al BCE, adjuntando la documentación que éste defina.

Artículo 4.- El BCE publicará periódicamente en su sitio web, el listado de las entidades autorizadas para operar como sistemas auxiliares de pagos.

Artículo 5.- La autorización conferida a las entidades para operar como sistemas auxiliares de pagos, no constituye garantía o certificación alguna por parte del BCE respecto de su capacidad legal, financiera y operativa, como tampoco representa garantía o certificación alguna sobre las operaciones de sus participantes.

De la supervisión y vigilancia

Artículo 6.- La supervisión que ejerza el BCE respecto de los sistemas de auxiliares de pagos, tendrá por objeto evaluar los mecanismos de control interno, el gobierno corporativo y la gestión riesgos a los que estén expuestos, sobre la base de los principios y estándares internacionales que aplican a las infraestructuras de pagos de los mercados financieros.

Artículo 7.- Corresponde al BCE la vigilancia del funcionamiento de los sistemas auxiliares de pagos que operan en el Ecuador, para lo cual recabará la información que considere relevante para valorar la eficiencia y seguridad de los sistemas e ¡instrumentos de pago que existen en el país.

De las medidas correctivas, infracciones y sanciones

Artículo 8.- El BCE en los términos y plazos establecidos en la normativa que dicte para el efecto, solicitará las medidas correctivas a los sistemas auxiliares de pagos que incumplan la normativa vigente.

Artículo 9.- El BCE aplicará las sanciones respectivas conforme lo dispuesto en el COMF.

Disposición general única. - El BCE ejercerá la vigilancia y supervisión de las entidades que operan como sistemas auxiliares de pagos para las actividades relacionadas con la liquidación y transferencias de recursos monetarios, por lo que las demás actividades a cargo de estas entidades, serán supervisadas por los organismos de control correspondientes.

2.4.6. Código Orgánico Monetario y Financiero

Según Código Orgánico Monetario y Financiero (2022) Suplemento del Registro Oficial 1, 11-II-2022 establece lo siguiente:

Artículo 26.- Naturaleza jurídica del Banco Central del Ecuador y normativa específica.

El Banco Central del Ecuador es una persona jurídica de derecho público, parte de la Función Ejecutiva, de duración indefinida, con autonomía institucional, administrativa, presupuestaria y técnica.

El Banco Central del Ecuador en el ejercicio de sus funciones y atribuciones se regirá por la Constitución de la República, este Código, su estatuto, las regulaciones expedidas por el órgano de gobierno, los reglamentos internos y las demás leyes aplicables en razón de la materia.

La instrumentación del régimen monetario le corresponde exclusivamente al Banco Central del Ecuador de conformidad con la Constitución de la República del Ecuador y las disposiciones de este Código.

Artículo 36.- Funciones.

El Banco Central del Ecuador tiene las siguientes funciones:

1.-Instrumentar la política en el ámbito monetario, para promover la sostenibilidad del sistema monetario y financiero de conformidad a las disposiciones de este Código;

2.-Elaborar y evaluar, en coordinación con el ente rector de las finanzas públicas y sin perjuicio de su autonomía, la programación macroeconómica en los sectores real, externo, monetario y financiero, validando su consistencia intersectorial con el sector fiscal;

3.-Elaborar informes de análisis de la proforma del Presupuesto General del Estado, que se presentará a la Asamblea Nacional;

4.-Elaborar y presentar los informes que le requiere la Junta de Política y Regulación Monetaria;

5.-Elaborar y emitir los informes de liquidez de la economía conforme lo dispone el artículo 119 de este Código.

6.-Elaborar un informe técnico anual respecto al nivel de la sostenibilidad de las reservas para operaciones de deuda, de acuerdo con lo previsto en el Código Orgánico de Planificación y Finanzas Públicas;

7.-Elaborar y publicar investigaciones y estadísticas de síntesis macroeconómica; así como investigaciones y estadísticas de los sistemas y medios de pago;

8.-Monitorear las tasas de interés con fines estadísticos;

9.-Preservar y administrar la reserva internacional y otros activos del Banco Central del Ecuador;

10.-Sin perjuicio de sus objetivos primarios, adquirir oro no monetario proveniente de la extracción de la pequeña minería y minería artesanal en el mercado nacional, de forma directa o por intermedio de agentes económicos públicos y privados, previamente autorizados por el propio Banco Central del Ecuador, así como la compra, venta y negociación de oro previo la autorización expresa de la Junta de Política y Regulación Monetaria;

11.-Actuar como administrador fiduciario de los Fideicomisos del Fondo de Liquidez de los Sectores Financieros Privado y Popular y Solidario; así como en fideicomisos exclusivamente enfocados en la instrumentación de política monetaria;

12.-Administrar el sistema central de pagos;

13.-Ejercer el control de los medios de pago; y, la vigilancia y supervisión de los sistemas auxiliares de pagos, fomentando la eficiencia, interoperabilidad e innovaciones en este ámbito;

14.-Actuar como agente fiscal, financiero y depositario de recursos públicos y proveer servicios bancarios a entidades del sector público y al sistema financiero nacional, de acuerdo a la remuneración de mercado que determine la Junta de Política y Regulación Monetaria;

15.-Determinar las características y gestionar la provisión, acuñación, circulación, canje, retiro y desmonetización de moneda fraccionaria;

16.- A nombre del Estado ecuatoriano, podrá contratar créditos externos para el financiamiento de la balanza de pagos y para atender necesidades de liquidez, con la aprobación del Comité de Deuda y Financiamiento;

17.- Actuar como depósito centralizado de compensación y liquidación de valores;

18.-Actuar como entidad de certificación electrónica;

19.-Ejercer la potestad sancionatoria de conformidad a la ley; y,

20.-Las demás que le asigne la ley.

Artículo 40.-Depósitos del sector público.

Los recursos públicos de las instituciones, organismos y empresas del sector público no financiero se mantendrán en depósito en el Banco Central del Ecuador, de conformidad con las regulaciones que emita la Junta de Política y Regulación Monetaria.

Las entidades del sistema financiero nacional y las calificadas dentro de los sistemas auxiliares de pago participarán en la recaudación de los recursos públicos, a través de cuentas recolectoras a nombre de las entidades públicas no financieras, de conformidad con las regulaciones que expida la Junta de Política y Regulación Monetaria. El saldo de dichas cuentas se transferirá a las cuentas que le corresponda a la respectiva institución pública en el Banco Central del Ecuador, de conformidad con la regulación que se expida para el efecto.

Las entidades del sistema financiero nacional no podrán abrir, a nombre de las instituciones públicas, otro tipo de cuentas, salvo que cuenten con la autorización otorgada por la Junta de Política y Regulación Monetaria, previo informe favorable del ente rector de las Finanzas públicas. Esta prohibición aplicará especialmente a las cuentas con capacidad de giro.

Las entidades del sistema financiero nacional identificarán de manera clara en sus registros la titularidad de las cuentas del inciso precedente y remitirán al Banco Central del Ecuador los saldos y movimientos que se realicen con cargo a aquellas, con la periodicidad que este determine.

Los sistemas auxiliares de pagos no podrán recaudar recursos públicos en cuentas propias.

El Banco Central del Ecuador sancionará la inobservancia o falta de cumplimiento a las disposiciones de este artículo como infracción grave.

Artículo 103.-Sistema nacional de pagos.

El sistema nacional de pagos comprende el conjunto de políticas, normas, instrumentos, procedimientos y servicios por medio de los cuales se efectúan, de

forma directa o indirecta, las transferencias de recursos gestionados a través de medios de pago y la liquidación de valores entre sus distintos participantes.

El sistema nacional de pagos está integrado por el sistema central de pagos y los sistemas auxiliares de pago. El Banco Central del Ecuador establecerá los requisitos de autorización, operación, registro y divulgación de la información de estos sistemas. El régimen tarifario correspondiente estará regulado por la Junta de Política y Regulación Monetaria.

Los informes que emitan los servidores y funcionarios del Banco Central del Ecuador, en el ejercicio de las funciones de supervisión del sistema nacional de pagos, serán escritos y reservados, así como los documentos que el Gerente General califique como tales, en virtud de precautelar la estabilidad del sistema. Estos informes no se divulgarán a terceros, en todo ni en parte, por el banco, por la entidad supervisada ni por ninguna persona que actúe por ellos, salvo cuando lo requiera la Junta de Política y Regulación Monetaria o cuando se ha determinado indicios de responsabilidad penal, que deberán ser denunciados a la Fiscalía General del Estado.

Artículo 109.- Supervisión de los sistemas auxiliares de pago.

El Banco Central del Ecuador efectuará la vigilancia y supervisión de los sistemas auxiliares de pagos y de sus entidades administradoras, así como de cualquier infraestructura de pagos o de transferencias de recursos monetarios que actúen en el mercado, para asegurar el correcto funcionamiento de los canales, instrumentos y medios de pago que se procesen por su intermedio.

La Junta de Política y Regulación Monetaria adoptará las regulaciones para determinar la operación, gobierno, control de riesgos y requerimientos financieros que los sistemas auxiliares de pago y sus agencias administradoras deben cumplir.

Los administradores de los sistemas auxiliares de pagos, incluyendo cualquier infraestructura de pagos o de transferencias de recursos monetarios, para su funcionamiento deberán contar con la autorización del Banco Central del Ecuador, y estarán obligados a remitir la información que este requiera y en los plazos que determine.

Esta información no se divulgará a terceros, en todo ni en parte, por el Banco Central del Ecuador, por la entidad supervisada ni por ninguna persona que actúe por ellos o que llegue a tener conocimiento de aquella por cualquier motivo, salvo cuando lo requiera la Junta de Política y Regulación Monetaria o cuando se haya determinado indicios de responsabilidad penal, que deberán ser denunciados a la Fiscalía General del Estado.

Artículo 110.-Medidas correctivas.

El banco central del ecuador dispondrá la aplicación de medidas correctivas a los sistemas de pagos auxiliares que hayan incumplido la normativa correspondiente.

Artículo 111.-Infracciones.

El Banco Central del Ecuador sancionará a las entidades a cargo de los sistemas auxiliares de pago y a sus administradores, cuando corresponda, por las siguientes causas:

1.-No ajustar la reglamentación interna a la normativa que emita la Junta de Política y Regulación Monetaria;

2.-No realizar las modificaciones a la reglamentación interna requeridas por el Banco Central del Ecuador dentro del plazo que se determine;

3.-Modificar los reglamentos internos sin contar con la autorización previa del Banco Central del Ecuador;

4.-No presentar la información que el Banco Central del Ecuador requiera o presentarla de manera imprecisa, incompleta o extemporánea;

5.-Proporcionar al Banco Central del Ecuador información falsa relacionada con el sistema de pagos respectivo;

6.-Realizar operaciones sin contar con la autorización del Banco Central del Ecuador;

7.-No cumplir con las disposiciones de interoperabilidad dispuestas por el Banco Central del Ecuador;

8.-Incumplir las medidas correctivas; y,

9.-Incumplir con cualquier otra obligación prevista en este Código o en la normativa que regule a los sistemas de pagos.

Las infracciones contenidas en los numerales 1, 2 y 3 serán consideradas graves. Las infracciones de los numerales 4, 5, 6, 7, 8 y 9 serán consideradas como muy graves.

Artículo 112.-Sanciones.

Por el cometimiento de las infracciones señaladas en el artículo precedente, el Banco Central del Ecuador impondrá las siguientes sanciones:

1.-Por las infracciones graves tipificadas en los numerales 1, 2 y 3 se aplicará una multa de hasta trescientos salarios básicos unificados; y,

2.-Por las infracciones muy graves tipificadas en los numerales 4, 5, 6, 7, 8 y 9 se aplicará una multa no menor de trescientos salarios básicos unificados, ni más de mil salarios básicos unificados.

Estas sanciones se aplicarán sin perjuicio de la obligación que tiene la entidad de subsanar el incumplimiento que motivó tal sanción. En caso de no subsanarse tal incumplimiento, el Banco Central del Ecuador solicitará a la superintendencia respectiva la remoción del correspondiente representante legal o, de ser el caso, suspenderá a la entidad en el sistema de pagos. La aplicación de estas sanciones no releva la responsabilidad directa de los administradores.

Artículo 113.-Sanción por operaciones sin autorización.

El Banco Central del Ecuador sancionará con una multa de hasta USD 800.000,00 (ochocientos mil dólares de los Estados Unidos de América), monto que será actualizado por la Junta de Política y Regulación Monetaria de conformidad con el índice de precios al consumidor, o hasta el nivel de ingresos del último ejercicio económico de la entidad, y la orden de suspensión inmediata de operaciones a las entidades que efectúen compensación o liquidación sin contar con la autorización respectiva.

2.5. Georreferencial

En el desarrollo del presente trabajo de investigación se tomó como punto de referencia a Ecuador, país del cual somos parte y, sobre todo, país en donde nuestro trabajo va enfatizar su investigación acerca de las seguridades de las transacciones en línea.

Ecuador tiene una extensión territorial de 256,370 km², y se encuentra en la línea ecuatorial en la parte noroeste de América del Sur. Limita al Norte con Colombia, al sur y al Este con Perú y al Oeste con el océano Pacífico. Sus regiones naturales son la región insular, donde se encuentra las islas Galápagos, situadas a 1,000 km al oeste de la costa ecuatoriana; la región sierra o andina, comprende toda la franja central del país en la que se encuentra el volcán Chimborazo, la costa, ocupa todo el litoral bañado por el océano Pacífico; y el oriente, que abarca la Amazonía ecuatoriana.

La organización política administrativa del Estado ecuatoriano comprende: el régimen seccional autónomo y el régimen dependiente del Ejecutivo. Administrativa y territorialmente el Ecuador se divide en 24 provincias, 7 en la Costa, 10 en la Sierra, 6 en la región Amazónica y 1 la región Insular. Las provincias se subdividen en cantones y éstos a su vez en parroquias urbanas y rurales.

Figura 5

Mapa Geográfico del Ecuador

Nota: El gráfico representa al mapa geográfico del Ecuador. Tomado de *Mapa Político del Ecuador*, por GoRaymi International TouristicPlatform S.A, 2022, Héroes del turismo.

CAPITULO III

METODOLOGÍA

3.1. Tipo de Investigación

La metodología que se aplicó en el presente trabajo de investigación corresponde con la investigación descriptiva. Porque se orienta a la caracterización de los elementos que integran el problema de investigación.

Carlos Sabino (1992) define a la investigación descriptiva como el tipo de investigación que tiene como objetivo describir algunas características fundamentales de conjuntos homogéneos de fenómenos, utilizando criterios sistemáticos que permiten establecer la estructura o el comportamiento de los fenómenos en estudio, proporcionando información sistemática y comparable con la de otras fuentes, por lo que se empleó en esta investigación haciendo uso de la descripción y análisis de las seguridades de las transacciones en línea en el Ecuador, Además esta investigación, puede servir de base para investigaciones que requieran un mayor nivel de profundidad en aspectos de amenazas, protocolos y certificaciones de seguridad de las transacciones en línea.

3.2. Enfoque de la investigación

3.2.1. Enfoque cualitativo

Según Blasco & Pérez (2007) señalan que "la investigación cualitativa estudia la realidad en su contexto natural y cómo sucede, sacando e interpretando fenómenos de acuerdo con las personas implicadas". Por lo expuesto se empleó este enfoque ya que se estudió y se analizó cuáles son las seguridades que tienen las transacciones en línea en el ecuador y cómo estas repercuten en la sociedad.

De igual manera el enfoque cualitativo permitió obtener datos que luego serán interpretados hermenéuticamente, como los criterios que cumplen con las seguridades de las transacciones en línea en el Ecuador, la cual se verá reflejada a través de fichas de observación.

3.3. Métodos de Investigación

En el presente trabajo de investigación se usó el método de investigación deductivo e inductivo debido a que se recopiló información y se analizaron cuáles son las seguridades de las transacciones en línea en el Ecuador, año 2022, con la finalidad de llegar a una conclusión el cual permitirá que los usuarios tengan una visión general de cómo repercuten las seguridades de las transacciones en línea en la sociedad.

3.3.1. Método inductivo

Se empleó este método para conocer e inducir cuales fueron los mecanismos y protocolos de seguridad que deben tener las transacciones en línea en el Ecuador.

3.3.2. Método deductivo

Mediante este método se buscó llegar a una deducción acerca de las implicaciones que tiene las seguridades en las transacciones en línea en el Ecuador, año 2022.

3.3.3. Método Bibliográfico

Este método se aplicó principalmente para buscar y recopilar información que ayudó a solventar nuestros objetivos específicos y a dar seguimiento a la investigación.

3.3.4. Método Documental

Se utilizó este método para realizar revisiones de documentos, libros, tesis, publicaciones entre otros, que aportan información sobre las seguridades de las transacciones en línea tanto para la identificación de problemas como para su análisis.

3.4. Técnicas e Instrumentos de Recopilación de Datos

Como técnica para la recolección de datos se empleó la ficha de observación no participante, ficha en la que se detalló las principales certificaciones y protocolos de seguridad que poseen las pasarelas de pago en el Ecuador.

En esta ficha los investigadores se mantienen al margen del fenómeno estudiado como un espectador pasivo que se limita a registrar la información que aparece ante

él, evitando la relación directa, pero pretendiendo obtener la máxima objetividad y veracidad posible.

El modelo y la estructura de la ficha de observación se encuentra definida por el nombre de la pasarela de pago, seguidamente por un listado de las certificaciones y protocolos de seguridad que se evaluó con un check list, para posteriormente obtener una ficha en donde se analizó el número total de certificaciones y protocolos de seguridad que cumplen y deducir el nivel de seguridad que poseen las pasarelas de pago.

3.5. Universo, Población y Muestra

3.5.1. Universo

El universo estudiado son todas las empresas que brindan el servicio de pasarelas de pago en el Ecuador, analizando las seguridades que proporcionan al momento de efectuar las transacciones en línea.

3.5.2. Población

La población estudiada está conformada por el total de las entidades que brindan el servicio de pasarelas de pago que se encuentran autorizadas por el Banco Central del Ecuador, siendo así un total de 7 entidades.

3.5.3. Muestra

Al contar con una población reducida de las entidades que brindan el servicio de pasarelas de pago en el Ecuador no se obtuvo ninguna muestra, sino que se estudió directamente al número total de las entidades.

3.6. Procesamiento de la Información

Una vez recopilada la información de diversas fuentes bibliográficas, documentales, se procedió analizar los resultados obtenidos de las fichas de observación, las cuales corresponden a identificar el nivel de seguridad que posee las pasarelas de pago, haciendo énfasis en sus certificaciones y protocolos de seguridad implementadas.

3.7. Aplicación de técnicas e instrumentos de investigación para la recopilación de información

3.7.1. Ficha de Observación

Se realizó siete fichas observación concerniente a: el número total de pasarelas de pago autorizadas por el Banco Central del Ecuador, las cuales son: Alignetsa S.A, Cardtech Ecuatoriana S.A, Ecuapayphone C.A, Kushki S.A. PagoPlux S.A, Paymentez (Nuvei), PlaceToPay.

3.8. Comprobación de la idea a defender

El estudio de la seguridad de las transacciones en línea, contribuirá a mejorar la seguridad en el comercio electrónico del Ecuador por lo que es importante saber cómo funcionan las transacciones por Internet y si son realmente seguras. Facilitando a la sociedad ecuatoriana en general la información acerca de las diferentes entidades de brindan el servicio de pasarela de pago y si estas cumplen con todos los parámetros de seguridad como son, certificación, protocolos y demás aspectos relevantes para que sean consideradas como plataformas seguras. Ayudando ya sea a centros comerciales como a los clientes a tener una visión general de que parámetros de seguridad poseen las entidades y cómo funcionan

3.9. Análisis de la información obtenida

Se trabajó con una estructura definida como las fichas de observación que permitió organizar la información de una manera clara y comprensible, por esta razón; cuenta con tres secciones: las certificaciones de seguridad, los protocolos de seguridad y las seguridades adicionales que son independientes, cada una de las variables contemplan a su vez varios parámetros para poder medir la seguridad que tienen las distintas entidades que brindan el servicio pasarelas de pago.

3.9.1. Ficha de Observación 1: Alignetsa S.A.

Mediante el instrumento utilizado (ficha de observación) en la fecha 10/08/2022 con el objetivo de analizar las seguridades en las transacciones en línea, corresponde a la pasarela de pago Alignetsa S.A, en la sección de las certificaciones de seguridad, cumplen con las siguientes certificaciones: Certificación PCI DSS, Certificación Visa, Certificación MasterCard, Certificación American Express y la

Certificación Diners Club, cuyas certificaciones brindan una medida de seguridad que permite la protección y la confidencialidad de los datos que se transmiten mediante la red. Se evidenció que no poseen las siguientes las certificaciones: Certificación Discover, Certificación Alia y la Certificación UnionPay.

En la sección de los protocolos y estándares de seguridad cumplen con los siguientes: Protocolo SSL (Secure Sockets Layer), Protocolo TLS (Transport Layer Security), Protocolo SET (Transacciones electrónicas seguras), Protocolo HTTPS (HyperText Transfer Protocol Secure), Protocolo 3D Secure, Monitoreo de Fraude, MasterCard SecureCode, Verified by Visa (VbV) estos protocolos de seguridad garantizan la confidencialidad, la integridad y la disponibilidad de la información. Es decir, son las medidas de seguridad implementadas para evitar que personas no autorizadas puedan acceder a la información, manipularlas o destruirlas.

En la sección de seguridades adicionales se evidenció que se encuentra implementado la autenticación basada en el EMV 3D Secure 2.1. Para más detalle dirigirse a los anexos ver ficha 1.

3.9.2 Ficha de Observación 2: Cardtech Ecuatoriana S.A.

Mediante el instrumento utilizado (ficha de observación) en la fecha 10/08/2022 con el objetivo de analizar las seguridades en las transacciones en línea, corresponde a la pasarela de pago Cardtech Ecuatoriana S.A, en la sección de las certificaciones de seguridad, cumplen con las siguientes certificaciones: Certificación PCI DSS, Certificación Visa, Certificación MasterCard y la Certificación American Express, cuyas certificaciones brindan una medida de seguridad que permite la protección y la confidencialidad de los datos que se transmiten mediante la red. Se evidenció que no poseen las siguientes las certificaciones: Diners Club, Certificación Discover, Certificación Alia y por último la Certificación UnionPay.

En la sección de los protocolos y estándares de seguridad cumplen con los siguientes: Protocolo SSL (Secure Sockets Layer), Protocolo TLS (Transport Layer Security), Protocolo SET (Transacciones electrónicas seguras), Protocolo HTTPS (HyperText Transfer Protocol Secure), Protocolo 3D Secure, Monitoreo de Fraude,

MasterCard SecureCode, Verified by Visa (VbV), estos protocolos de seguridad garantizan la confidencialidad, la integridad y la disponibilidad de la información. Es decir, son las medidas de seguridad implementadas para evitar que personas no autorizadas puedan acceder a la información, manipularlas o destruirlas.

En la sección de seguridades adicionales se evidenció que se encuentra implementado las Políticas del sistema integrado de gestión (SIG). Para más detalle dirigirse a los anexos ver ficha 2.

3.9.3 Ficha de Observación 3: Ecuapayphone C.A.

Mediante el instrumento utilizado (ficha de observación) en la fecha 10/08/2022 con el objetivo de analizar las seguridades en las transacciones en línea, corresponde a la pasarela de pago Ecuapayphone C.A, en la sección de las certificaciones de seguridad, cumplen con las siguientes certificaciones: Certificación PCI DSS, Certificación Visa y la Certificación MasterCard, cuyas certificaciones brindan una medida de seguridad que permite la protección y la confidencialidad de los datos que se transmiten mediante la red. Se evidenció que no poseen las siguientes las certificaciones: Certificación American Express, Certificación Diners Club, Certificación Discover, Certificación Alia y por último la Certificación UnionPay.

En la sección de los protocolos y estándares de seguridad cumplen con los siguientes: Protocolo SSL (Secure Sockets Layer), Protocolo TLS (Transport Layer Security), Protocolo SET (Transacciones electrónicas seguras), Protocolo HTTPS (HyperText Transfer Protocol Secure), Protocolo 3D Secure, Monitoreo de Fraude, MasterCard SecureCode, Verified by Visa (VbV), estos protocolos de seguridad garantizan la confidencialidad, la integridad y la disponibilidad de la información. Es decir, son las medidas de seguridad implementadas para evitar que personas no autorizadas puedan acceder a la información, manipularlas o destruirlas.

En la sección de seguridades adicionales se evidenció que se encuentra implementado como método de seguridad el motor antifraude SEON y el control de seguimiento de las transacciones en línea. Para más detalle dirigirse a los anexos ver ficha 3.

3.9.4 Ficha de Observación 4: Kushki S.A.

Mediante el instrumento utilizado (ficha de observación) en la fecha 10/08/2022 con el objetivo de analizar las seguridades en las transacciones en línea, corresponde a la pasarela de pago Kushki S.A, en la sección de las certificaciones de seguridad, cumplen con las siguientes certificaciones: Certificación PCI DSS, Certificación Visa, Certificación MasterCard, Certificación American Express y la Certificación Alia, cuyas certificaciones brindan una medida de seguridad que permite la protección y la confidencialidad de los datos que se transmiten mediante la red. Se evidenció que no poseen las siguientes las certificaciones: Certificación Diners Club, Certificación Discover y la Certificación UnionPay.

En la sección de los protocolos y estándares de seguridad cumplen con los siguientes: Protocolo SSL (Secure Sockets Layer), Protocolo TLS (Transport Layer Security), Protocolo SET (Transacciones electrónicas seguras), Protocolo HTTPS (HyperText Transfer Protocol Secure), Protocolo 3D Secure, Monitoreo de Fraude, MasterCard SecureCode, Verified by Visa (VbV), estos protocolos de seguridad garantizan la confidencialidad, la integridad y la disponibilidad de la información. Es decir, son las medidas de seguridad implementadas para evitar que personas no autorizadas puedan acceder a la información, manipularlas o destruirlas.

En la sección de seguridades adicionales se evidenció que se encuentra implementado Tokenización, Machine learning, Puntaje transaccional y Autenticación de doble factor. Para más detalle dirigirse a los anexos ver ficha 4.

3.9.5 Ficha de Observación 5: PagoPlux S.A.

Mediante el instrumento utilizado (ficha de observación) en la fecha 10/08/2022 con el objetivo de analizar las seguridades en las transacciones en línea, corresponde a la pasarela de pago PagoPlux S.A, en la sección de las certificaciones de seguridad, cumplen con las siguientes certificaciones: Certificación PCI DSS, Certificación Visa, Certificación MasterCard, Certificación Diners Club y la Certificación Discover, cuyas certificaciones brindan una medida de seguridad que permite la protección y la confidencialidad de los datos que se transmiten mediante la red. Se evidenció que no poseen las siguientes las certificaciones: Certificación American Express, Certificación Alia y la Certificación UnionPay

En la sección de los protocolos y estándares de seguridad cumplen con los siguientes: Protocolo SSL (Secure Sockets Layer), Protocolo TLS (Transport Layer Security), Protocolo SET (Transacciones electrónicas seguras), Protocolo HTTPS (HyperText Transfer Protocol Secure), Protocolo 3D Secure, Monitoreo de Fraude, MasterCard SecureCode, Verified by Visa (VbV), estos protocolos de seguridad garantizan la confidencialidad, la integridad y la disponibilidad de la información. Es decir, son las medidas de seguridad implementadas para evitar que personas no autorizadas puedan acceder a la información, manipularlas o destruirlas.

En la sección de seguridades adicionales se evidenció que se encuentra implementado Validación one time password (OTP), Motor antifraude ACI ReD Shield, Verificación de Correo electrónico, Verificación de identidad KYC (Know Your Customer). Para más detalle dirigirse a los anexos ver ficha 5.

3.9.6 Ficha de Observación 6: Paymentez (Nuvei)

Mediante el instrumento utilizado (ficha de observación) en la fecha 10/08/2022 con el objetivo de analizar las seguridades en las transacciones en línea, corresponde a la pasarela de pago Paymentez (Nuvei), en la sección de las certificaciones de seguridad, cumplen con las siguientes certificaciones: Certificación PCI DSS, Certificación Visa, Certificación MasterCard, Certificación American Express, Certificación Diners Club, Certificación Discover, Certificación Alia y la Certificación UnionPay, cuyas certificaciones brindan una medida de seguridad que permite la protección y la confidencialidad de los datos que se transmiten mediante la red.

En la sección de los protocolos y estándares de seguridad cumplen con los siguientes: Protocolo SSL (Secure Sockets Layer), Protocolo TLS (Transport Layer Security), Protocolo SET (Transacciones electrónicas seguras), Protocolo HTTPS (HyperText Transfer Protocol Secure), Protocolo 3D Secure, Monitoreo de Fraude, MasterCard SecureCode, Verified by Visa (VbV), estos protocolos de seguridad garantizan la confidencialidad, la integridad y la disponibilidad de la información. Es decir, son las medidas de seguridad implementadas para evitar que personas no autorizadas puedan acceder a la información, manipularlas o destruirlas.

En la sección de seguridades adicionales se evidenció que se encuentra implementado la Tecnología EMV (tarjeta con chip), Cifrado punto a punto (P2PE), Tokenización, EKYC y gestión de identidad, Gestión de contracargos. Para más detalle dirigirse a los anexos ver ficha 6.

3.9.7 Ficha de Observación 7: PlaceToPay.

Mediante el instrumento utilizado (ficha de observación) en la fecha 10/08/2022 con el objetivo de analizar las seguridades en las transacciones en línea, corresponde a la pasarela de pago PlaceToPay, en la sección de las certificaciones de seguridad, cumplen con las siguientes certificaciones: Certificación PCI DSS, Certificación Visa, Certificación MasterCard, Certificación American Express, Certificación Diners Club, Certificación Discover, y la Certificación Alia, cuyas certificaciones brindan una medida de seguridad que permite la protección y la confidencialidad de los datos que se transmiten mediante la red. Se evidenció que no poseen las siguientes las certificaciones: Certificación American Express, Certificación Alia y la Certificación UnionPay

En la sección de los protocolos y estándares de seguridad cumplen con los siguientes: Protocolo SSL (Secure Sockets Layer), Protocolo TLS (Transport Layer Security), Protocolo SET (Transacciones electrónicas seguras), Protocolo HTTPS (HyperText Transfer Protocol Secure), Protocolo 3D Secure, Monitoreo de Fraude, MasterCard SecureCode, Verified by Visa (VbV), estos protocolos de seguridad garantizan la confidencialidad, la integridad y la disponibilidad de la información. Es decir, son las medidas de seguridad implementadas para evitar que personas no autorizadas puedan acceder a la información, manipularlas o destruirlas.

En la sección de seguridades adicionales se evidenció que se encuentra implementado 3DS Placetopay, Servicio de verificación de direcciones (AVS), Sistema modular de control de fraude (Scudo), Análisis histórico y Revisión manual. Para más detalle dirigirse a los anexos ver ficha 7.

Haciendo un análisis a las pasarelas de pago en el Ecuador podemos notar que la mayoría cumplen con casi todas las certificaciones y protocolos de seguridad que garantizan su eficiencia, siendo así que existen pasarelas de pagos destacadas como

Paymentez que a su vez viene a ser la que mejor calificada. Dando lugar a realizar un breve análisis de su funcionamiento dentro del mercado ecuatoriano.

Paymentez permite a los comercios en Ecuador recibir pagos de tarjetas de crédito, débito y prepago, integrados con todas en un solo clic, cuenta con más de 5 millones de clientes ofreciendo transferencias bancarias y pagos en efectivo con más de 60 mil transacciones diarias, Permite diferir compras y pagos completamente seguros en transacciones online, porque cumplen con los estándares internacionales de seguridad de datos y todo esto desde el dispositivo de su preferencia, tienen herramientas para monitoreo anti fraude, certificado de seguridad PCI/DSS y complementos, al estar enlazados con switches transaccionales, por lo que son la primera plataforma en aceptar tarjetas de débito y prepago en ecuador.

¿Cómo funciona Paymentez?

Ronald quiere comprar un pan de pascua en el sitio web de un comercio local TIA, cuando Ronald realiza su compra online la transacción se conecta con los servidores deprimentes, la transacción de Ronald pasa por los filtros de seguridad y es analizada por el sistema anti fraude, el banco aprueba la transacción y Ronald recibe su confirmación de compra inmediatamente, Ronald compró de forma segura fácil y rápida y el establecimiento aumentó sus ventas online.

Figura 6

Proceso sobre cómo funcionan las pasarelas de pago en una compra en línea.

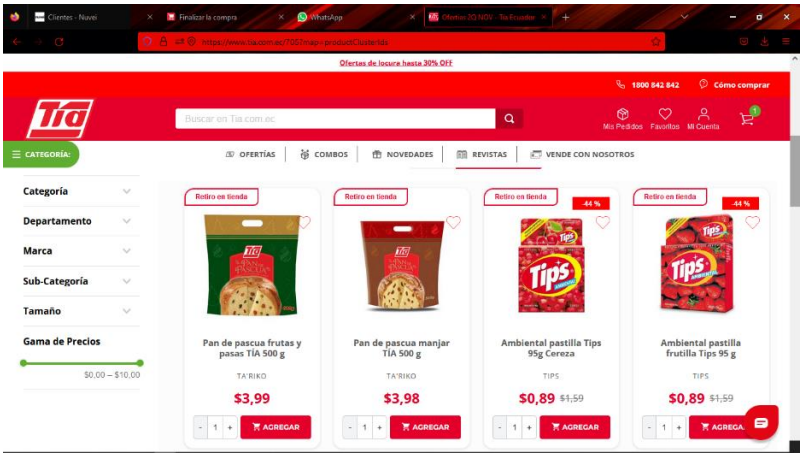
Nota. Transacción de compra a través de Paymentez. por Ayme & Sanda, 2022.

3.9.8 Análisis del caso

Cuando un cliente entra en una tienda online, recordemos que debe asegurarse de que la tienda es segura accediendo por HTTPS, y decide adquirir algún producto o servicio.

Figura 7

Tienda online TIA

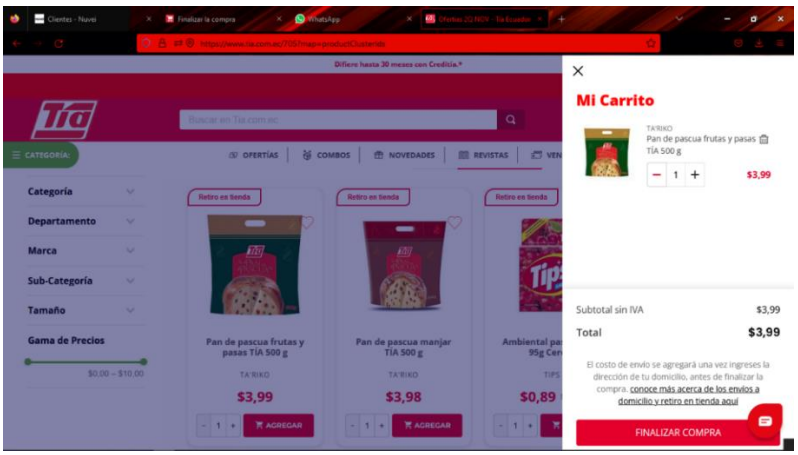


Nota. Interfaz de la tienda online TIA. Tomado de *página oficial de Tia*, por Ayme & Sanda, 2022.

En la figura 7, se muestra la página principal de la tienda online TIA que dispone de una variedad de productos, donde el cliente tiene a su disposición y voluntad de poder seleccionarlos.

Figura 8

Selección de productos

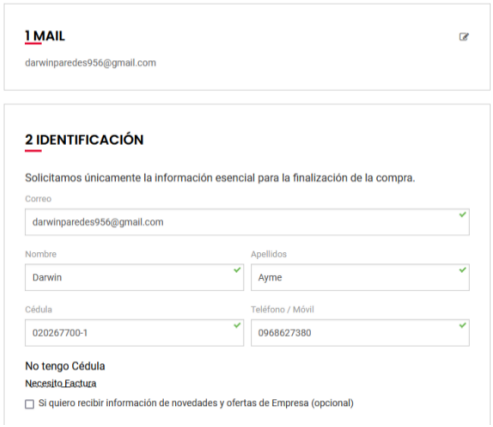


Nota. Seleccionar los productos que se desea adquirir. Tomado de *página oficial de Tia*, por Ayme & Sanda, 2022.

En la figura 8, se muestra que una vez seleccionada el producto deseado se procede a enviarlo al carrito de compra.

Figura 9

Datos de identificación



Nota. Datos de identificación para la compra del producto. Tomado de *página oficial de Tia*, por Ayme & Sanda, 2022.

En este momento, el navegador del cliente cifra la comunicación TLS, de esta forma, se evita que la comunicación pueda ser interceptada y modificada por un ciberdelincuente.

Figura 10

Puntos de retiro

Nota. Dirección de los puntos de retiro de nuestro producto. Tomado de *página oficial de Tia*, por Ayme & Sanda, 2022.

En la figura 10, muestra las opciones de envió a domicilio como también los puntos de retiros más cercanos, haciendo uso de la geolocalización de nuestro dispositivo e indicando la sucursal más cercana.

Figura 11

Opciones de pago

Nota. Opciones de pago con tarjetas de crédito, débito y transferencias bancarias. Tomado de *página oficial de Tia*, por Ayme & Sanda, 2022.

Una vez asegurada la conexión, el cliente procede a indicar sus datos bancarios a la tienda online mediante la pasarela de pago, estos datos, se envían al banco del vendedor para su comprobación. Una vez comprobados los datos del comprador, el banco envía los detalles de la comprobación de nuevo a la tienda online, e indica al cliente que los datos han sido correctamente verificados y que se ha autorizado a continuar con el proceso de compra.

Figura 12

Ingreso de datos bancarios

Nota. Ingreso de los datos correspondientes a la tarjeta de débito. Tomado de *página oficial de Tia*, por Ayme & Sanda, 2022.

A continuación, el banco del cliente, la entidad del vendedor remite los datos de la operación a la del comprador, si todo es correcto, la entidad del comprador autoriza la operación y remite un mensaje al banco del vendedor, que será recibido por la pasarela de pago, autorizando finalmente la operación de compra. Si hubiera algún error durante todo el proceso, la pasarela recibiría la información, mostrando los mensajes pertinentes.

Figura 13

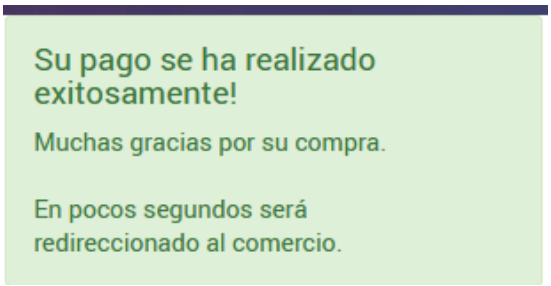
Código de seguridad

Nota. Código de seguridad para comprobar la autenticidad del comprador. Tomado de *página oficial de Tia,* por Ayme & Sanda, 2022.

En la figura 13, se solicita un código de seguridad que es enviado al correo electrónico con la cual se encuentra registrado la tarjeta o a su vez un SMS al número telefónico registrado a nombre del propietario de la tarjeta de débito.

Figura 14

Pago exitoso



Nota. Pago realizado exitosamente. Tomado de la *página oficial de Tia*, por Ayme & Sanda, 2022.

Puede parecer un proceso largo, pero todo se realiza en escasos segundos y de forma segura, como podemos apreciar, las pasarelas de pago no son más que intermediarios que controlan que la operación cumpla unas garantías de seguridad para ambas partes; por tanto, cuanto más segura y fiable es una pasarela de pago, mejor es la experiencia del cliente en la tienda online

3.10. Generación de conclusiones y Recomendaciones

3.10.1. Conclusión

El comercio electrónico va creciendo en el Ecuador exponencialmente. Cada vez más empresas ven el mundo digital como la mejor manera de vender y llegar a su público por lo que es importante revisar, analizar los componentes, mecanismos y seguridades que poseen las pasarelas de pago en Ecuador. Para que se tome la mejor decisión y poder implementarlo. El estudio de las pasarelas de pago se estructuró haciendo uso de las fichas de observación en donde se plasmó las características relevantes en varios aspectos relacionados a venta, logística y seguridad.

3.10.2. Recomendación

La elección de una buena pasarela de pagos que satisfaga las necesidades y las de sus clientes es fundamental y son muchos aspectos los que se deben tomar en cuenta al momento de analizarlas como son: flexibilidad, certificaciones, estabilidad, entre otros. Puesto que la pasarela de pagos no solo será el medio por el que se perciben las ganancias de la empresa si no también que debe ser una plataforma 100% confiable ya que manejará datos financieros de los clientes y es vital darles confianza y transparencia al momento de realizar sus pagos.

Es por ello que en base al estudio realizado se recomienda que Paymentez (Nuvei) es la pasarela de pago ideal, debido a que cuenta con todas las certificaciones además tiene implementado la mayoría de los protocolos y mecanismos de seguridad que les permite poseer una alta protección de los datos, evitando que la información se exponga de manera pública y se pueda ser utilizada para ciberdelitos y usos fraudulentos, mencionar también que trabajan con la mayoría de las tarjetas de crédito, débito facilitando a los clientes la disponibilidad del servicio.

CAPITULO IV

RESULTADOS Y DISCUSIÓN

4.1. Análisis, Interpretación y Discusión de Resultados

El análisis e interpretación de resultados sobre las pasarelas de pago avaladas por el Banco Central del Ecuador: Alignetsa S.A., Cardtech Ecuatoriana S.A, Ecuapayphone C.A, Kushki S.A, PagoPlux S.A, Paymentez (Nuvei) y PlaceToPay, forman parte de un cambio importante para el desarrollo del comercio electrónico en el Ecuador, debido a que funcionan y trabajan como un puente entre el banco y el comprador, proporcionando seguridad al momento que se realiza la transacción, por lo que analizar las seguridades que poseen las pasarelas de pago van a facilitar a una mejor comprensión de como las seguridades funcionan en este proceso. Estas herramientas fundamentales en los negocios e-Commerce ofrecen seguridad y confianza a las transacciones en línea. Funcionan como TPV virtuales, que autorizan los pagos por tarjeta de crédito o débito desde aplicaciones web o móviles. Hablamos de plataformas que facilitan el pago telemático a través de Internet. Aunque existen muchas similitudes hay diferencias entre una pasarela de pagos y otra como se muestra a continuación.

Tabla 5

Cuadro comparativo de las pasarelas de pago

CUADRO COMPARATIVO DE LAS PASARELAS DE PAGO ECUADOR 2022							
PASARELAS DE PAGO	**PROTOCOLOS DE SEGURIDAD**	**CERTIFICACIONES DE SEGURIDAD**	**CLIENTES**	**TARIFAS POR SERVICIO**	**TARJETAS ACEPTADAS**	**CARACTERÍSTICAS**	**SEGURIDAD**
Alignetsa S.A.	• Protocolo SSL. • Protocolo TLS. • Protocolo SET. • Protocolo HTTPS. • Protocolo 3D Secure. • Monitoreo de Fraude. • MasterCard SecureCode. • Verified by Visa.	• Certificación PCI DSS. • Certificación Visa. • Certificación MasterCard. • Certificación American Express. • Certificación Diners Club. **ADICIONALES** Autenticación basada en el EMV 3D Secure 2.1	PACIFICARD Banco Guayaquil Produbanco Grupo Promerica Banco del Austro Banco Pichincha Banco Boliviano. Banco Internacional Banco de Machala. CLARO. LATAM AIRLINES MOVISTAR. PEPSICO SCANIA. RIPLEY	Tarifa de USD 0.35 (treinta y cinco centavos) más los impuestos de ley por concepto de recaudación de fondos públicos, que aplicarán los SAP a sus clientes.	VISA MASTERCARD AMERICAN EXPRESS DINERS CLUB.	Brinda el servicio OTP, que incluye los nuevos enfoques de autenticación exigidos por EMV, que son: Biometría, Push Notificación sin costos adicionales. Además, tiene la capacidad de hacer adecuaciones a la medida del cliente, los precios se manejan acorde con el mercado. La plataforma de autenticación se encuentra certificada por las marcas internacionales de tarjeta de crédito. Los usuarios pueden realizar compras fuera del país, ya que el mensaje OTP puede llegarles a través de un SMS o correo electrónico autenticado.	MEDIA

			SODIMAC			Cuenta con el Know How para implementar los esquemas de autenticación basados en RBA (Rules Based Authentication) e Identity Check.	
Cardtech Ecuatoriana S.A.	• Protocolo SSL. • Protocolo TLS. • Protocolo SET. • Protocolo HTTPS. • Protocolo 3D Secure. • Monitoreo de Fraude. • MasterCard SecureCode. • Verified by Visa.	• Certificación PCI DSS. • Certificación Visa. • Certificación MasterCard. • Certificación American Express. **ADICIONALES** Políticas del Sistema Integrado de Gestión (SIG)	SCANIA. RIPLEY SODIMAC INDURAMA DIFARE	Tarifa de USD 0.35 (treinta y cinco centavos) más los impuestos de ley por concepto de recaudación de fondos públicos, que aplicarán los SAP a sus clientes.	VISA MASTERCARD AMERICAN EXPRESS	Brinda servicios de personalización de tarjetas financieras servicio de arrendamiento y venta de ATMs.	MEDIA
Ecuapayphone C.A.	• Protocolo SSL. • Protocolo TLS.	• Certificación PCI DSS. • Certificación Visa.	VITAPRO TOYOTA LAS FRAGANCIAS INDURAMA	Tarifa de USD 0.35 (treinta y cinco centavos) más los impuestos de ley por concepto de recaudación de fondos públicos,	VISA MASTERCARD DE PRODUBANCO	Brinda una sección de desarrolladores que permite integrar el botón de pagos en una página web desde el backend y si la página web está sobre Wordpress, Prestashop,	MEDIA

	• Protocolo SET. • Protocolo HTTPS. • Protocolo 3D Secure. • Monitoreo de Fraude • MasterCard SecureCode • Verified by Visa.	• Certificación MasterCard **ADICIONALES** • Motor antifraude SEON • Control de transacciones	DIFARE GRUPASA SUMESA. BAGO CONTINENTAL.	que aplicarán los SAP a sus clientes.		Shopify o Magento se puede integrar fácilmente. Sistema de pagos instantáneo basado en el uso de smartphones,	
Kushki S.A.	• Protocolo SSL. • Protocolo TLS. • Protocolo SET. • Protocolo HTTPS. • Protocolo 3D Secure. • Monitoreo de Fraude.	• Certificación PCI DSS. • Certificación Visa. • Certificación MasterCard. • Certificación American Express. • Certificación Alia. **ADICIONALES**	CLARO. TWENTY NETLIFE WOM AWTO INDRIVER SEGUROS LA EQUIDAD.	Tarifa de USD 0.35 (treinta y cinco centavos) más los impuestos de ley por concepto de recaudación de fondos públicos, que aplicarán los SAP a sus clientes.	VISA MASTERCARD AMERICAN EXPRESS ALIA	Facilidad para cobrar a través de una plataforma a la población no bancarizada, además de ofrecer sus redes de pago internacional en efectivo La implementación puede tomar al menos dos meses. Se tiene que hacer un contrato con cada banco, lo que implica papeleo y requisitos.	MEDIA

	• MasterCard. SecureCode. • Verified by Visa.	• Tokenización. • Machine learning. • Puntaje transaccional. • Autenticación de doble factor	UNIVERSIDAD DE LAS AMÉRICAS ECUADOR. RAPPI SURA				
PagoPlux S.A.	• Protocolo SSL. • Protocolo TLS. • Protocolo SET. • Protocolo HTTPS. • Protocolo 3D Secure. • Monitoreo de Fraude. • MasterCard SecureCode . • Verified by Visa.	• Certificación PCI DSS. • Certificación Visa. • Certificación MasterCard. • Certificación Diners Club. • Certificación Discover. **ADICIONALES** • Validación one time password (OTP).	SQUARESPACE PRESTASHOP MAGENTO ODOO VTEX OPENCART WOO COMERCE YELO	Tarifa de USD 0.35 (treinta y cinco centavos) más los impuestos de ley por concepto de recaudación de fondos públicos, que aplicarán los SAP a sus clientes.	VISA MASTERCARD AMEX DINERS CLUB DISCOVER	PagoPlux, permite de una forma fácil, rápida y segura realizar los pagos a sus colaboradores, clientes, proveedores a través de tarjetas prepago recargables. Automatiza el proceso de emisión de facturas ahorrando tiempo y esfuerzo cuando reciben un pago digital. Se integra a los sistemas de la empresa o negocio**:** ERP, POS, BPMs, CRM, Kioskos, sistemas contables, softwares médicos y más. Plataforma de pagos multicanal (WhatsApp,	MEDIA

		• Motor antifraude ACI ReD Shield. • Verificación de Correo electrónico. • Verificación de identidad KYC (Know Your Customer)				redes sociales, WEB, e-mail) para empresas y negocios que permite cobrar de forma fácil, rápida y segura Ahorra costos y optimiza los procesos fácilmente al incorporarlos a sus canales comerciales con tecnología robusta y versátil.	
Paymentez (Nuvei)	• Protocolo SSL. • Protocolo TLS. • Protocolo SET. • Protocolo HTTPS. • Protocolo 3D Secure. • Monitoreo de Fraude. • MasterCard SecureCode.	• Certificación PCI DSS. • Certificación Visa. • Certificación MasterCard. • Certificación American Express. • Certificación Diners Club. • Certificación Discover.	PYCA SAMSUNG COMANDATO PICKER SONY TIA CREDITOS ECONOMICOS. LA GANGA TESALIA ABC BURGER KING ETAFASHION TIPTI	Tarifa de USD 0.35 (treinta y cinco centavos) más los impuestos de ley por concepto de recaudación de fondos públicos, que aplicarán los SAP a sus clientes.	VISA MASTERCARD AMERICAN EXPRESS DINERS CLUB DISCOVER, ALIA UNIONPAY	Paymentez permite que el cliente pueda diferir sus compras en la misma plataforma y su diseño está adaptado y enfocado hacia la función más que al aspecto visual. Tienen actualmente el primer botón de pago rápido, ágil y seguro del país, y cuya alianza estratégica con Banco del Pacifico. One Click Buy y toda la seguridad de la compra es respaldada por Paymentez Ecuador y Banco del Pacifico.	ALTA

	• Verified by Visa.	• Certificación Alia. • Certificación UnionPay. **ADICIONALES** • Tecnología EMV (tarjeta con chip). • Cifrado punto a punto (P2PE). • Tokenización . • EKYC y gestión de identidad. • Gestión de contracargos.	TICKETSHOW HERBALIFE WHIRLPOOL GRUPOHINODE MARCIMEX FARMACIAS MEDICITY			Realiza los cobros desde whatsapp y correo. Vende desde cualquier red social. Permite a los clientes que realicen los pagos de forma rápida y segura a través de un código QR. Ofrece planes y membresías de todos los servicios y realiza cobros de forma automática. permite realizar facturas electrónicas autorizadas por el SRI de forma automática una vez realizado el pago	
PlaceToPay	• Protocolo SSL. • Protocolo TLS. • Protocolo SET.	• Certificación PCI DSS. • Certificación Visa. • Certificación MasterCard. • Certificación American Express.	PYCA SAMSUNG COMANDATO PICKER SONY	Tarifa de USD 0.35 (treinta y cinco centavos) más los impuestos de ley por concepto de recaudación de fondos públicos, que aplicarán los SAP a sus clientes.	VISA MASTERCARD AMERICAN EXPRESS DINERS CLUB DISCOVERY	Los productos principales son un botón de pagos para incorporarlo en la página web de la empresa y un enlace de cobro para aquellas que no disponen de páginas web. Reduce el riesgo de fraude a través de servicios virtuales que se	ALTA

	• Protocolo HTTPS. • Protocolo 3D Secure. • Monitoreo de Fraude. • MasterCard SecureCode. • Verified by Visa.	• Certificación Diners Club. • Certificación Discover. • Certificación Alia. **ADICIONALES** • 3DS Placetopay. • Servicio de verificación de direcciones • Sistema de control de fraude (Scudo). • Análisis histórico.			ALIA	adaptan a las necesidades del negocio. Cuenta con integración a los principales CMS y frameworks. En cuanto al dinero, ofrece dos alternativas: modelo gateway, el dinero llega directamente a tu cuenta o modelo agregador, el dinero llega a Place to pay y luego se transfiere a la cuenta del negocio	

Nota: Esta tabla muestra un cuadro comparativo de las pasarelas de pago del Ecuador.

Diariamente a través de las pasarelas de pago se procesa un gran volumen de transacciones en línea y hay que resaltar que el éxito de toda tienda Online se centra en generar confianza y seguridad a los usuarios para que estos compren sin temor a través de la web. Integrar en el e-Commerce las pasarelas de pago adecuadas para los clientes es fundamental, en el cuadro comparativo se indica características de cada una de ellas. Ahora que se conoce las certificaciones y protocolos de seguridad que se ha implementado en las pasarelas de pago autorizadas por el Banco Central del Ecuador, solo nos toca descubrir cuál es la que mejor que se adapte a la empresa para empezar disfrutar de todas las ventajas. Como se puede ver, es importante darle prioridad a la seguridad de los usuarios y así poder elegir una pasarela que cuente con toda la documentación y certificaciones necesarias.

CONCLUSIONES

La presente investigación permitió realizar un estudio de todas las seguridades que existen actualmente en las transacciones en línea a través de las pasarelas de pago, permitiendo indicar que cualquiera de ellas cumple con las normas y estándares básicas que rige el Banco Central del Ecuador para brindar un servicio seguro, esperando que los usuarios se sientan satisfechos sobre las reglas, normas y estándares que establece la entidad para resguardar la información.

Existen varios tipos de amenazas que tratan de comprometer a las transacciones en línea, su propósito es aprovechar alguna vulnerabilidad para atacar. En cuanto a las amenazas, las más frecuentes de hoy en día son el Pishing, Pharming, Smishing, Vishing, Key logger, Skimming, Adware, Spyware, que mediante la suplantación de identidad el ciberdelincuente se hace pasar por una persona o entidad para adquirir información de forma fraudulenta. Sin embargo, así como existen varios tipos de amenazas, también hay varios mecanismos y protocolos de seguridad que garantizan que una transacción en línea sea segura.

Las principales causas que impiden a las transacciones en línea y el comercio electrónico alcanzar su potencial máximo son la desconfianza y el miedo a la falta de seguridad en el envío y recepción de datos. Uno de los medios que trata de evitar esta traba son los protocolos de seguridad, que son soluciones tecnológicas que buscan asegurar que los datos relativos a una transacción en línea puedan ser transmitidos de forma segura. Los protocolos de seguridad más generalizados son el SSL, SET, TLS, HTTPS. El estudio de los distintos protocolos de seguridad utilizados a día de hoy deja claro que la seguridad en todos ellos está verificada y se han realizado avances para proteger los datos.

En Ecuador existe varias empresas que brindan el servicio de las pasarelas de pago sin embargo en esta investigación se centró en las empresas autorizadas por el Banco Central del Ecuador que son denominadas Sistemas Auxiliares de Pago, en total son 7 entidades, encargadas de concluir con el proceso de transacciones entre los bancos y las empresas contratantes, las mismas que tienen un número de seguridades que permiten dar confianza al usuario.

Según el Código Orgánico Monetario y Financiero, el Banco Central del Ecuador tiene la función de ejercer el control de los medios de pago; y, la vigilancia y supervisión de los sistemas auxiliares de pagos, para su funcionamiento deberán contar con la autorización del Banco Central del Ecuador, y estarán obligados a remitir la información que este requiera y en los plazos que determine, los requisitos para la autorización de las entidades que prestan el servicio de pasarelas de pago son el Certificado de Estándar de Seguridad de Datos para la Industria de Tarjeta de Pago PCI DSS o estándares ISO para pagos y otros servicios financieros. Por lo tanto, las entidades que brindan este servicio cumplen con la certificación PCI DSS, dado que es requisito primordial para ser calificado como una entidad Administradoras de los Sistemas Auxiliares de Pago.

RECOMENDACIONES

Se recomienda que en futuros trabajos de investigación, se aplique trabajos prácticos cumpliendo las normas vigentes del Banco Central del Ecuador a través de las pasarelas de pago, debido a que brinda la posibilidad de que lo sectores involucrados en el comercio electrónico, conozcan la ley, su alcance y significado e ilustrar eficacia sobre el uso adecuado de las transacciones en línea.

La creciente popularidad del comercio electrónico y el uso de las transacciones en línea, ha dado lugar a un aumento en las actividades maliciosas de los ciberdelincuentes, por tal motivo se recomienda mantener actualizados todos los sistemas operativos y programas de software mediante la instalación de actualizaciones con regularidad en los sistemas de seguridad tan pronto estén disponibles en los terminales de los usuarios.

Todos los protocolos que existen actualmente para asegurar la información sensible de los usuarios son efectivos si se implementan de manera correcta, por lo que se recomienda combinarlos y usar más de uno para garantizar un nivel alto de seguridad.

En Ecuador existen varias entidades que brinda el servicio de pasarelas de pago, pero se recomienda adquirir este servicio de las entidades que son reguladas por el Banco Central del Ecuador ya que el artículo 111 del Código Orgánico referido, establece las causales por las que el Banco Central del Ecuador sancionará a las entidades a cargo de los sistemas auxiliares de pagos y a sus administradores.

Existen diversas amenazas en la seguridad de las transacciones en línea y tanto las entidades que brindan el servicio de pasarelas de pago como los usuarios que acceden a estos servicios son responsables de minimizar los peligros que siempre existirán. Frente a esto se recomienda que toda organización que procese, transmita o almacene datos de tarjetas de pago deben cumplir con los requerimientos que establece la norma PCI DSS.

BIBLIOGRAFÍA

Aciworldwide. (2021). *Gestión de fraude de ACI para comerciantes*. https://www.aciworldwide.com/solutions/aci-fraud-management-merchants

Alignet. (2022). *Estándares de seguridad*. https://www.alignet.com/ams/

Applus Laboratories. (2022). *Certificación Mastercard*. https://www.appluslaboratories.com/global/es/what-we-do/service-sheet/certificaci%C3%B3n-mastercard

Araujo, A. (2021). *¿Qué es PCI DSS y quiénes deben cumplirla?* https://blog.hackmetrix.com/que-es-pci-dss/

Banco Central del Ecuador. (2022). *Resolución Administrativa Nro. BCE-GG-007-2022*. https://www.bce.ec/images/transparencia2022/documental/BCE-GG-007-2022.pdf

Banco Solidario. (2018). *Porque nos importa*. https://www.banco-solidario.com/conocenos/negocio-social

Barros, J. (2010). *Implementación de un prototipo de tienda virtual sobre plataforma Linux para realizar transacciones de comercio electrónico seguro* [Universidad de Cuenca]. https://dspace.ucuenca.edu.ec/bitstream/123456789/2530/1/tm4396.pdf

Blasco, J., & Pérez, J. (2007). *Metodologías de investigación en educación física y deportes: ampliando horizontes* [Universidad de Alicante]. http://hdl.handle.net/10045/12270

Buch, J., & Jordán, F. (2022). *La seguridad de las transacciones bancarias en internet*. http://www.conganat.org/SEIS/informes/2001/PDF/6BuchTarrats.pdf

Cámara Ecuatoriana de Comercio Electrónico. (2021). *¡Ecuador vive un gran crecimiento en eCommerce!* https://cece.ec/ecuador-vive-un-gran-crecimiento-en-ecommerce/#:~:text=La%20Superintendencia%20de%20Bancos%20de,a%20trav%C3%A9s%20de%20pagos%20digitales.

Cárdenas, W., & Petro, A. (2022). *Pasarelas de Pago al Servicio del E-commerce en las Empresas de Streaming*. https://repositorio.unicordoba.edu.co/bitstream/handle/ucordoba/5122/cardenasmejiawendi-petromartinezandrea.pdf?sequence=1&isAllow

Cardtech. (2021). *Cardtech*. https://www.cardtechcorp.com/nosotros/

Castro, C. (2017). *Modelo de seguridad para garantizar la integridad de los pagos móviles basados en near field communication (nfc)* [Escuela Superior

Politécnica de Chimborazo]. http://dspace.espoch.edu.ec/bitstream/123456789/7842/1/20T00952.pdf

Código Orgánico Monetario y Financiero. (2022). *Suplemento del Registro Oficial 1, 11-II-2022*. https://biblioteca.defensoria.gob.ec/bitstream/37000/3399/1/C%c3%b3digo%20Org%c3%a1nico%20Monetario%20y%20Financiero.pdf

Computerworld. (2022). *¿Qué es el skimming de tarjetas?* https://cso.computerworld.es/tendencias/target-comparte-su-propia-herramienta-de-deteccion-de-skimming-web

Congreso Nacional. (2014). *Código orgánico integral penal, Coip*. https://www.defensa.gob.ec/wp-content/uploads/downloads/2021/03/COIP_act_feb-2021.pdf

Congreso Nacional. (2022). *Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos*. https://www.gob.ec/regulaciones/ley-comercio-electronico-firmas-mensajes-datos

Constitución de la República del Ecuador. (2015). *Registro Oficial 449 de 20-oct.-2008*. https://www.cosede.gob.ec/wp-content/uploads/2019/08/CONSTITUCION-DE-LA-REPUBLICA-DEL-ECUADOR.pdf

Diners Club. (2022). *Protección de Datos*. https://www.dinersclub.com.ec/aviso-de-la-politica-de-privacidad

eCommerce Institute. (2022). *Empresas Finalistas eCommerce Awards Ecuador 2022*.

Electronic IDentification. (2022). *KYC (Know Your Customer): qué es y su actualidad 2022*. https://www.electronicid.eu/es/blog/post/que-es-kyc-know-customer/es

Erazo, M., & Montenegro, R. (2005). *Sistema de control de transacciones en cajas y cajeros automáticos mediante la captura de imágenes*. http://repositorio.espe.edu.ec/xmlui/bitstream/handle/21000/849/T-ESPE-014093.pdf?sequence=1&isAllowed=y

Evertec. (2022). *Seguridad*.

GcfGlobal. (2022). *Transacciones financieras seguras en internet*. https://edu.gcfglobal.org/es/seguridad-en-internet/transacciones-financieras-seguras-en-internet/1/

GlobeNewswire. (2021). *Nuvei compra Paymentez y continúa su expansión en el mercado latinoamericano*. https://www.globenewswire.com/news-release/2021/09/07/2292358/0/es/Nuvei-compra-Paymentez-y-

contin%C3%BAa-su-expansi%C3%B3n-en-el-mercado-latinoamericano.html

Jara, K. (2020). *Análisis sobre las seguridades en las transacciones electrónicas dentro del comercio electrónico* [Universidad Técnica de Machala]. http://repositorio.utmachala.edu.ec/handle/48000/15896

Junta de Política y Regulación Monetaria y Financiera, (2018). https://www.bce.fin.ec/images/junta/Resolucion-441-2018-M.pdf?dl=0

Kaspesrky. (2022). *¿Qué es el adware?* https://latam.kaspersky.com/resource-center/threats/adware

Kruger. (2021). *PagoPlux: Integra botones de pago con máxima productividad*. https://blog.krugercorp.com/pagopluxintegrabotonesdepago

Kushki. (2018). *Combate el fraude y protégete a ti y a tus clientes*.

López, D., & Redchuk, A. (2016). *Tendencias sociales en el comercio electrónico de América Latina: a propósito de los proveedores adheridos a códigos de buenas prácticas*. https://produccioncientificaluz.org/index.php/opcion/article/view/20613/20523

Manotoa, M. (2021). *Elementos fundamentales para el diseño de una regulación que considere la prevención del lavado de activos en el uso de las pasarelas de pago en el Ecuador*. https://repositorio.uasb.edu.ec/bitstream/10644/8206/1/T3591-MDFBS-Manotoa-Elementos.pdf

Merino, A. (2015). *Análisis de factibilidad de la creación de una revista electrónica de deportes enfocada a la población de 15 a 30 años, de clase media alta y alta, de la ciudad de Quito* [Universidad San Francisco de Quito]. https://repositorio.usfq.edu.ec/bitstream/23000/4879/1/120961.pdf

Ministerio de Telecomunicaciones y de la Sociedad de la Información. (2020). *Estrategia nacional de comercio electrónico*.

Molina, D. (2007). *Seguridades en Comercio Electrónico* [Universidad del Azuay]. https://dspace.uazuay.edu.ec/bitstream/datos/2286/1/05805.pdf

Navarro, J., Ubilla, G., & Tejeda, M. (2014). *Redes de Computadores*. http://profesores.elo.utfsm.cl/~agv/elo322/1s14/projects/reports/G5/Informe%20TLS.pdf

Nuvei. (2022). *Cumplimiento y seguridad*. https://nuvei.com/company/compliance-security/

Organización de Naciones Unidas. (2017). *Conferencia de las Naciones Unidas sobre Comercio y Desarrollo*. http://www.oecd-ilibrary.org/industry-and-services/oecd-recommendation-of-the-

Orús, A. (2022). *Comercio electrónico en el mundo - Datos estadísticos*. https://es.statista.com/temas/9072/comercio-electronico-en-el-mundo/#topicHeader__wrapper

PagoPlux. (2022). *Un aliado que te da seguridad 24/7*. https://www.pagoplux.com/inicio/

Parrilla, L. (2015). *E-commerce y pago seguro*. https://core.ac.uk/download/pdf/44310168.pdf

Ponce, J. (2021). *Estado digital Ecuador 2021*. https://blog.formaciongerencial.com/estadodigitalecuador2021/

Redesna. (2022). *¿Qué es Spyware?* http://www.redesna.com/Archivos/6.-SpyWare.pdf

Ryte. (2021). *Protocolo HTTPS (protocolo de Transferencia de Hiper-Texto)*. https://es.ryte.com/wiki/HTTPS

Sabogal, C. (2021). *Análisis de la seguridad informática en las transacciones electrónicas para el comercio electrónico* [Universidad Nacional Abierta y a Distancia Especialización en Seguridad Informática]. https://repository.unad.edu.co/bitstream/handle/10596/44132/ccsabogal.pdf?sequence=1&isAllowed=y

Salas, D. (2010). *La Seguridad en las Transacciones en el Comercio Electrónico*. Corporación Universitaria de la Costa.

Saúl, C. (2015). *Comercio Electrónico: Importancia de la Seguridad en las Transacciones Electrónicas, Amenazas y Soluciones a Implementar*.

SEON Technologies. (2022). *Gestión del Fraude Realmente Potente*. https://learn.seon.io/es-sistema-de-deteccion-de-fraude?utm_term=antifraude&utm_campaign=%5BS%5D%20Fraud%20prevention%20%5BES%5D%20%5BLATAM%5D&utm_source=google&utm_medium=cpc&hsa_acc=9508664392&hsa_cam=12816168617&hsa_grp=122618829338&hsa_ad=614317488213&hsa_src=g&hsa_tgt=kwd-304092830116&hsa_kw=antifraude&hsa_mt=p&hsa_net=adwords&hsa_ver=3&gclid=Cj0KCQjw0oyYBhDGARIsAMZEuMvR48cVMkV4mCYGTGEz8LZGX8NOcmbu0UCERzjKhzi-UtKbNMtED_YaAkvYEALw_wcB

Sifone. (2002). *Validación OTP*. https://www.sifonecompany.com/site/validacion-otp/

Tello, P., & Pineda, L. (2017). *Análisis del comercio electrónico en Ecuador*. Universidad Internacional del Ecuador.

UnionPay. (2020). *Reglas de Certificación*. https://cert.unionpay.com/cert-portal-en/authenticate/rule/

Validity. (2021). *¿Qué es la verificación de correo electrónico y por qué es importante?* https://www.validity.com/es/todo-sobre-la-verificacion-de-correo-electronico/#:~:text=La%20verificaci%C3%B3n%20de%20correo%20electr%C3%B3nico%20garantiza%20que%20las%20direcciones%20de,direcciones%20de%20correo%20electr%C3%B3nico%20incorrectas.

Villatoro, R. (2015). *Seguridad en las transacciones en línea de comercio electrónico*. Universidad Don Bosco.

Visa. (2022). *Nuestra principal prioridad es protegerte*. https://www.visa.com.ar/products/visa-secure.html

ANEXOS

Cronograma (Gantt)

	CRONOGRAMA DE ACTIVIDADES				JUNIO					JULIO					AGOSTO					SEPTIEMBRE					OCTUBRE				
	Estudio de las seguridades de las transacciones en línea en el ecuador, año 2022.				SEMANAS					SEMANAS					SEMANAS					SEMANAS					SEMANAS				
		Responsable	INICIO	FINAL	1	2	3	4	5	1	2	3	4	5	1	2	3	4	5	1	2	3	4	5	1	2	3	4	5
n	ACTIVIDADES																												
1	Denuncia del tema	Autores	13-Jun	13-Jun																									
2	Realización del planteamiento del problema.	Autores	13-Jun	13-Jun																									
3	Elaboración del problema de investigación.	Autores	14-Jun	14-Jun																									
4	Elaboración de las preguntas de Investigación.	Autores	14-Jun	14-Jun																									
5	Desarrollo de la Justificación, Objetivos e Idea a defender.	Autores	15-Jun	17-Jun																									
6	Investigación documental del Marco teórico.	Autores	20-Jun	20-Jun																									
7	Realizar los antecedentes.	Autores	20-Jun	20-Jun																									
8	Realizar el Marco Científico.	Autores	21-Jun	21-Jun																									
9	Realizar el Marco Conceptual.	Autores	21-Jun	21-Jun																									
10	Realizar el Marco Legal.	Autores	22-Jun	22-Jun																									
11	Realizar el Marco Georreferencial.	Autores	23-Jun	23-Jun																									
12	Elaboración de la Metodología de la Investigación, Métodos, población y muestra.	Autores	24-Jun	24-Jun																									
13	Elaboración de los instrumentos de investigación.	Autores	25-Jun	30-Jun																									
14	Identificar las empresas que brindan el servicio de pasarelas de pago existen en el Ecuador	Autores	1-Jul	15-Jul																									
15	Investigar si las empresas de pasarela de pagos cumplen con la certificación PCI DSS.	Autores	18-Jul	29-Jul																									
16	Identificar los protocolos de seguridad que se aplican para una transacción en línea segura.	Autores	1-Aug	12-Aug																									
17	Identificar cuáles son los diferentes tipos de amenazas de las transacciones en línea.	Autores	15-Aug	20-Aug																									
18	Realizar las fichas de observación de cada una de las pasarelas de pago del Ecuador.	Autores	21-Aug	27-Aug																									
19	Realizar un cuadro comparativo de las pasarelas de pago con sus características resaltantes.	Autores	28-Aug	5-Sep																									
20	Mencionar si los resultados obtenidos cumples con la idea a defender expuesta.	Autores	6-Sep	30-Sep																									
21	Plasmar las conclusiones y recomendaciones	Autores	1-Oct	14-Oct																									
22	Revisión y Corrección de errores del borrador del proyecto de investigación.	Autores	15-Oct	27-Oct																									
23	Presentación Final.	Autores	28-Oct	28-Oct																									

Presupuesto Ejecutado

DESCRIPCIÓN	DETALLE	CANTIDAD	VALOR UNITARIO	VALOR TOTAL
Recursos Humanos	Personal	2	0	0
	Movilización	16	0,30	4,80
	Alimentación	16	2,50	40,00
Recursos Materiales	Materiales de Oficina	1	40,00	40,00
	Impresora	1	60,00	60,00
	Copias	3	6,00	18,00
	Anillados	3	0,75	2,25
	Empastado	3	2,00	6,00
	Cd	2	5,00	10,00
Otros	Internet	3	25,00	75,00
	Laptop	1	900,00	900,00
			TOTAL	**1156,05**

Instrumentos de recopilación de datos

Ficha 1 Alignetsa S.A.

Ficha de observación			
Objetivo	Análisis de seguridades	**Fecha**	10/08/2022
Pasarela de pagos	Alignetsa S.A	**Observadores**	Darwin Ayme Ronald Sanda

No	**Certificaciones de seguridad**	**Cumple**	**No cumple**
1	Certificación PCI DSS	✓	
2	Certificación Visa	✓	
3	Certificación MasterCard	✓	
4	Certificación American Express	✓	
5	Certificación Diners Club	✓	
6	Certificación Discover		✓
7	Certificación Alia		✓
8	Certificación UnionPay		✓
	Protocolos y Estándares de seguridad		
1	Protocolo SSL (Secure Sockets Layer)	✓	
2	Protocolo TLS (Transport Layer Security)	✓	
3	Protocolo SET (Transacciones electrónicas seguras)	✓	
4	Protocolo HTTPS (HyperText Transfer Protocol Secure)	✓	
5	Protocolo 3D Secure	✓	
6	Monitoreo de Fraude	✓	
7	MasterCard SecureCode	✓	
8	Verified by Visa (VbV)	✓	
	Seguridades Adicionales		
1	Autenticación basada en el EMV 3D Secure 2.1	✓	

Observaciones:
Las certificaciones de tarjetas financieras son emitidas por las franquicias Visa, MasterCard, etc. El objeto de la certificación son las empresas dedicadas a la producción, fabricación, operación y gestión de tarjetas financieras, implementarán la evaluación de acceso, la evaluación de procesos, la supervisión posterior a la certificación y otros controles y gestión de cumplimiento de normas técnicas.
El comercio electrónico necesita garantizar la seguridad de las transacciones en línea, en este sentido se han plasmado una serie de seguridades que brindan las pasarelas de pago en el Ecuador, en donde se va ir verificando que protocolos y estándares cumplen las distintas pasarelas de pago, para evitar los posibles peligros u operaciones ilegales a los que puede estar sometida las transacciones en línea. Básicamente se trataría de garantizar el uso de las mismas.

Ficha 2 Cardtech Ecuatoriana S.A.

Ficha de observación				
Objetivo	Análisis de seguridades	**Fecha**	10/08/2022	
Pasarela de pago	Cardtech Ecuatoriana S.A.	**Observadores**	Darwin Ayme Ronald Sanda	
No	**Certificaciones de seguridad**		**Cumple**	**No cumple**
1	Certificación PCI DSS		✓	
2	Certificación Visa		✓	
3	Certificación MasterCard		✓	
4	Certificación American Express		✓	
5	Certificación Diners Club			✓
6	Certificación Discover			✓
7	Certificación Alia			✓
8	Certificación UnionPay			✓
	Protocolos y Estándares de seguridad			
1	Protocolo SSL (Secure Sockets Layer)		✓	
2	Protocolo TLS (Transport Layer Security)		✓	
3	Protocolo SET (Transacciones electrónicas seguras)		✓	
4	Protocolo HTTPS (HyperText Transfer Protocol Secure)		✓	
5	Protocolo 3D Secure		✓	
6	Monitoreo de Fraude		✓	
7	MasterCard SecureCode		✓	
8	Verified by Visa (VbV)		✓	
	Seguridades Adicionales			
1	Políticas del Sistema Integrado de Gestión (SIG)		✓	

Observaciones:

Las certificaciones de tarjetas financieras son emitidas por las franquicias Visa, MasterCard, etc. El objeto de la certificación son las empresas dedicadas a la producción, fabricación, operación y gestión de tarjetas financieras, implementarán la evaluación de acceso, la evaluación de procesos, la supervisión posterior a la certificación y otros controles y gestión de cumplimiento de normas técnicas.

El comercio electrónico necesita garantizar la seguridad de las transacciones en línea, en este sentido se han plasmado una serie de seguridades que brindan las pasarelas de pago en el Ecuador, en donde se va ir verificando que protocolos y estándares cumplen las distintas pasarelas de pago, para evitar los posibles peligros u operaciones ilegales a los que puede estar sometida las transacciones en línea. Básicamente se trataría de garantizar el uso de las mismas.

Ficha 3 Ecuapayphone C.A.

Ficha de observación				
Objetivo	Análisis de seguridades	**Fecha**	10/08/2022	
Pasarela de pago	Ecuapayphone C.A.	**Observadores**	Darwin Ayme Ronald Sanda	
No	**Certificaciones de seguridad**		**Cumple**	**No cumple**
1	Certificación PCI DSS		✓	
2	Certificación Visa		✓	
3	Certificación MasterCard		✓	
4	Certificación American Express			✓
5	Certificación Diners Club			✓
6	Certificación Discover			✓
7	Certificación Alia			✓
8	Certificación UnionPay			✓
	Protocolos y Estándares de seguridad			
1	Protocolo SSL (Secure Sockets Layer)		✓	
2	Protocolo TLS (Transport Layer Security)		✓	
3	Protocolo SET (Transacciones electrónicas seguras)		✓	
4	Protocolo HTTPS (HyperText Transfer Protocol Secure)		✓	
5	Protocolo 3D Secure		✓	
6	Monitoreo de Fraude		✓	
7	MasterCard SecureCode		✓	
8	Verified by Visa (VbV)		✓	
	Seguridades Adicionales			
1	Motor antifraude SEON		✓	
2	Control de transacciones		✓	

Observaciones:
Las certificaciones de tarjetas financieras son emitidas por las franquicias Visa, MasterCard, etc. El objeto de la certificación son las empresas dedicadas a la producción, fabricación, operación y gestión de tarjetas financieras, implementarán la evaluación de acceso, la evaluación de procesos, la supervisión posterior a la certificación y otros controles y gestión de cumplimiento de normas técnicas.
El comercio electrónico necesita garantizar la seguridad de las transacciones en línea, en este sentido se han plasmado una serie de seguridades que brindan las pasarelas de pago en el Ecuador, en donde se va ir verificando que protocolos y estándares cumplen las distintas pasarelas de pago, para evitar los posibles peligros u operaciones ilegales a los que puede estar sometida las transacciones en línea. Básicamente se trataría de garantizar el uso de las mismas.

Ficha 4 Kushki S.A.

Ficha de observación			
Objetivo	Análisis de seguridades	**Fecha**	10/08/2022
Pasarela de pago	Kushki S.A.	**Observadores**	Darwin Ayme Ronald Sanda

No	Certificaciones de seguridad	Cumple	No cumple
1	Certificación PCI DSS	✓	
2	Certificación Visa	✓	
3	Certificación MasterCard	✓	
4	Certificación American Express	✓	
5	Certificación Diners Club		✓
6	Certificación Discover		✓
7	Certificación Alia	✓	
8	Certificación UnionPay		✓
	Protocolos y Estándares de seguridad		
1	Protocolo SSL (Secure Sockets Layer)	✓	
2	Protocolo TLS (Transport Layer Security)	✓	
3	Protocolo SET (Transacciones electrónicas seguras)	✓	
4	Protocolo HTTPS (HyperText Transfer Protocol Secure)	✓	
5	Protocolo 3D Secure	✓	
6	Monitoreo de Fraude	✓	
7	MasterCard SecureCode	✓	
8	Verified by Visa (VbV)	✓	
	Seguridades Adicionales		
1	Tokenización	✓	
2	Machine learning	✓	
3	Puntaje transaccional	✓	
4	Autenticación de doble factor	✓	

Observaciones:
Las certificaciones de tarjetas financieras son emitidas por las franquicias Visa, MasterCard, etc. El objeto de la certificación son las empresas dedicadas a la producción, fabricación, operación y gestión de tarjetas financieras, implementarán la evaluación de acceso, la evaluación de procesos, la supervisión posterior a la certificación y otros controles y gestión de cumplimiento de normas técnicas.
El comercio electrónico necesita garantizar la seguridad de las transacciones en línea, en este sentido se han plasmado una serie de seguridades que brindan las pasarelas de pago en el Ecuador, en donde se va ir verificando que protocolos y estándares cumplen las distintas pasarelas de pago, para evitar los posibles peligros u operaciones ilegales a los que puede estar sometida las transacciones en línea. Básicamente se trataría de garantizar el uso de las mismas.

Ficha 5 PagoPlux S.A.

Ficha de observación			
Objetivo	Análisis de seguridades	**Fecha**	10/08/2022
Pasarela de pagos	PagoPlux S.A.	**Observadores**	Darwin Ayme Ronald Sanda

No	Certificaciones de seguridad	Cumple	No cumple
1	Certificación PCI DSS	✓	
2	Certificación Visa	✓	
3	Certificación MasterCard	✓	
4	Certificación American Express		✓
5	Certificación Diners Club	✓	
6	Certificación Discover	✓	
7	Certificación Alia		✓
8	Certificación UnionPay		✓
	Protocolos y Estándares de seguridad		
1	Protocolo SSL (Secure Sockets Layer)	✓	
2	Protocolo TLS (Transport Layer Security)	✓	
3	Protocolo SET (Transacciones electrónicas seguras)	✓	
4	Protocolo HTTPS (HyperText Transfer Protocol Secure)	✓	
5	Protocolo 3D Secure	✓	
6	Monitoreo de Fraude	✓	
7	MasterCard SecureCode	✓	
8	Verified by Visa (VbV)	✓	
	Seguridades Adicionales		
1	Validación One Time Password (OTP)	✓	
2	Motor antifraude ACI ReD Shield	✓	
3	Verificación de Correo electrónico	✓	
4	Verificación de identidad KYC (Know Your Customer)	✓	

Observaciones:

Las certificaciones de tarjetas financieras son emitidas por las franquicias Visa, MasterCard, etc. El objeto de la certificación son las empresas dedicadas a la producción, fabricación, operación y gestión de tarjetas financieras, implementarán la evaluación de acceso, la evaluación de procesos, la supervisión posterior a la certificación y otros controles y gestión de cumplimiento de normas técnicas.

El comercio electrónico necesita garantizar la seguridad de las transacciones en línea, en este sentido se han plasmado una serie de seguridades que brindan las pasarelas de pago en el Ecuador, en donde se va ir verificando que protocolos y estándares cumplen las distintas pasarelas de pago, para evitar los posibles peligros u operaciones ilegales a los que puede estar sometida las transacciones en línea. Básicamente se trataría de garantizar el uso de las mismas.

Ficha 6 Paymentez (Nuvei)

Ficha de observación			
Objetivo	Análisis de seguridades	**Fecha**	10/08/2022
Pasarela de pago	Paymentez (Nuvei)	**Observadores**	Darwin Ayme Ronald Sanda

No	Certificaciones de seguridad	Cumple	No cumple
1	Certificación PCI DSS	✓	
2	Certificación Visa	✓	
3	Certificación MasterCard	✓	
4	Certificación American Express	✓	
5	Certificación Diners Club	✓	
6	Certificación Discover	✓	
7	Certificación Alia	✓	
8	Certificación UnionPay	✓	
	Protocolos y Estándares de seguridad		
1	Protocolo SSL (Secure Sockets Layer)	✓	
2	Protocolo TLS (Transport Layer Security)	✓	
3	Protocolo SET (Transacciones electrónicas seguras)	✓	
4	Protocolo HTTPS (HyperText Transfer Protocol Secure)	✓	
5	Protocolo 3D Secure	✓	
6	Monitoreo de Fraude	✓	
7	MasterCard SecureCode	✓	
8	Verified by Visa (VbV)	✓	
	Seguridades Adicionales		
1	Tecnología EMV (tarjeta con chip)	✓	
2	Cifrado punto a punto (P2PE)	✓	
3	Tokenización	✓	
4	EKYC y gestión de identidad	✓	
5	Gestión de contracargos	✓	

Observaciones:

Las certificaciones de tarjetas financieras son emitidas por las franquicias Visa, MasterCard, etc. El objeto de la certificación son las empresas dedicadas a la producción, fabricación, operación y gestión de tarjetas financieras, implementarán la evaluación de acceso, la evaluación de procesos, la supervisión posterior a la certificación y otros controles y gestión de cumplimiento de normas técnicas.

El comercio electrónico necesita garantizar la seguridad de las transacciones en línea, en este sentido se han plasmado una serie de seguridades que brindan las pasarelas de pago en el Ecuador, en donde se va ir verificando que protocolos y estándares cumplen las distintas pasarelas de pago, para evitar los posibles peligros u operaciones ilegales a los que puede estar sometida las transacciones en línea. Básicamente se trataría de garantizar el uso de las mismas.

Ficha 7 PlaceToPay

Ficha de observación			
Objetivo	Análisis de seguridades	**Fecha**	10/08/2022
Pasarela de pago	PlaceToPay	**Observadores**	Darwin Ayme Ronald Sanda

No	Certificaciones de seguridad	Cumple	No cumple
1	Certificación PCI DSS	✓	
2	Certificación Visa	✓	
3	Certificación MasterCard	✓	
4	Certificación American Express	✓	
5	Certificación Diners Club	✓	
6	Certificación Discover	✓	
7	Certificación Alia	✓	
8	Certificación UnionPay		✓
	Protocolos y Estándares de seguridad		
1	Protocolo SSL (Secure Sockets Layer)	✓	
2	Protocolo TLS (Transport Layer Security)	✓	
3	Protocolo SET (Transacciones electrónicas seguras)	✓	
4	Protocolo HTTPS (HyperText Transfer Protocol Secure)	✓	
5	Protocolo 3D Secure	✓	
6	Monitoreo de Fraude	✓	
7	MasterCard SecureCode	✓	
8	Verified by Visa (VbV)	✓	
	Seguridades Adicionales		
1	3DS Placetopay	✓	
2	Servicio de verificación de direcciones (AVS)	✓	
3	Sistema modular de control de fraude (Scudo)	✓	
4	Análisis histórico	✓	
5	Revisión manual	✓	

Observaciones:

Las certificaciones de tarjetas financieras son emitidas por las franquicias Visa, MasterCard, etc. El objeto de la certificación son las empresas dedicadas a la producción, fabricación, operación y gestión de tarjetas financieras, implementarán la evaluación de acceso, la evaluación de procesos, la supervisión posterior a la certificación y otros controles y gestión de cumplimiento de normas técnicas.

El comercio electrónico necesita garantizar la seguridad de las transacciones en línea, en este sentido se han plasmado una serie de seguridades que brindan las pasarelas de pago en el Ecuador, en donde se va ir verificando que protocolos y estándares cumplen las distintas pasarelas de pago, para evitar los posibles peligros u operaciones ilegales a los que puede estar sometida las transacciones en línea. Básicamente se trataría de garantizar el uso de las mismas.

Certificado de Anti plagio

CERTIFICADO

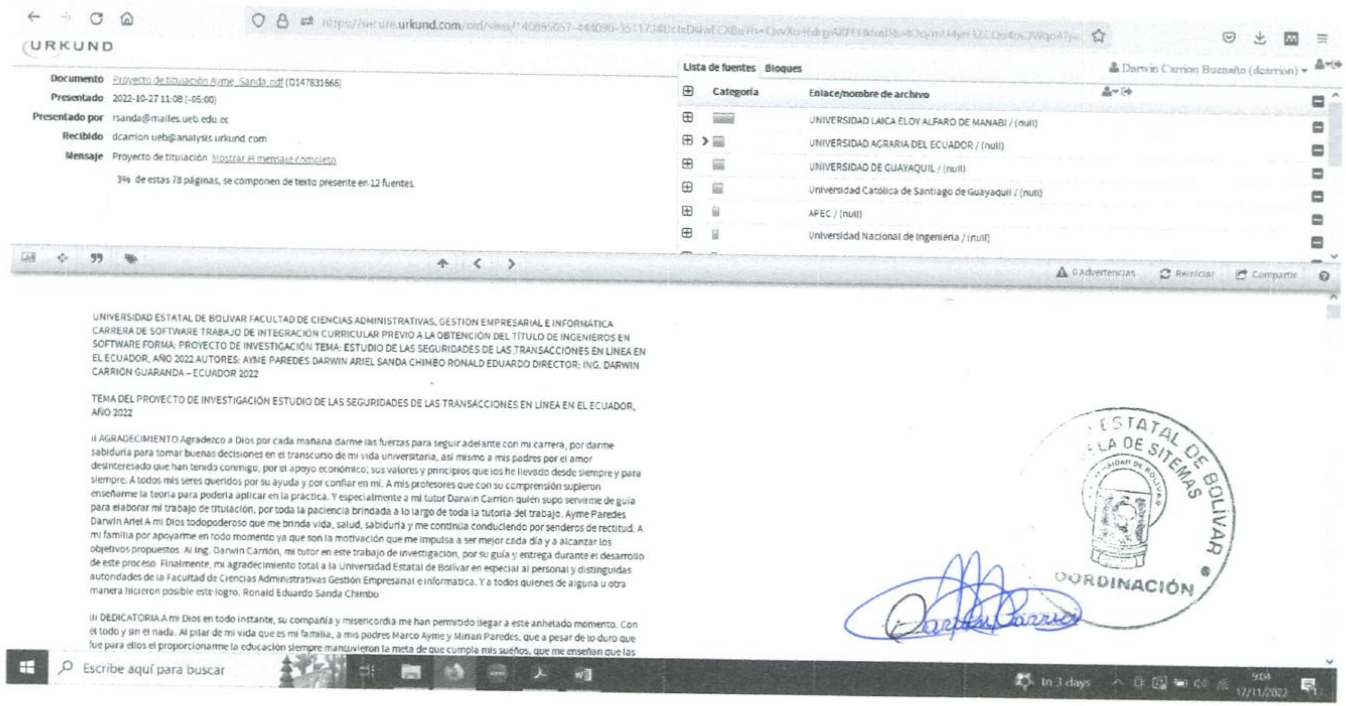
Yo, DARWIN PAUL CARRIÓN BUENAÑO con C.I. 0603021395 certifico que se ha cumplido con la revisión del informe final del trabajo de titulación "ESTUDIO DE LAS SEGURIDADES DE LAS TRANSACCIONES EN LÍNEA EN EL ECUADOR, AÑO 2022" a través de la herramienta URKUND el 27 de octubre del 2022, proyecto de autoría de los Srs. AYME PAREDES DARWIN ARIEL SANDA CHIMBO RONALD EDUARDO, dando como resultado del 3% de coincidencia no accidental, porcentaje que está dentro del parámetro permitido.

Guaranda, 17 de noviembre del 2022.

Atentamente

ING. DARWIN CARRIÓN BUENAÑO

DIRECTOR TRABAJO DE TITULACIÓN


URKUND
Documento Proyecto de titulación Ayme_Sanda.pdf (D147831666)
Presentado 2022-10-27 11:08 (-05:00)
Presentado por rsanda@mailes.ueb.edu.ec
Recibido dcarrion.ueb@analysis.urkund.com
Mensaje Proyecto de titulación Mostrar el mensaje completo
3% de estas 78 páginas, se componen de texto presente en 12 fuentes.
Lista de fuentes Bloques
Darwin Carrion Buenaño (dcarrion)
Categoría
Enlace/nombre de archivo
UNIVERSIDAD LAICA ELOY ALFARO DE MANABI / (null)
UNIVERSIDAD AGRARIA DEL ECUADOR / (null)
UNIVERSIDAD DE GUAYAQUIL / (null)
Universidad Católica de Santiago de Guayaquil / (null)
APEC / (null)
Universidad Nacional de Ingeniería / (null)
0 Advertencias
Reiniciar
Compartir
UNIVERSIDAD ESTATAL DE BOLÍVAR FACULTAD DE CIENCIAS ADMINISTRATIVAS, GESTIÓN EMPRESARIAL E INFORMÁTICA CARRERA DE SOFTWARE TRABAJO DE INTEGRACIÓN CURRICULAR PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIEROS EN SOFTWARE FORMA: PROYECTO DE INVESTIGACIÓN TEMA: ESTUDIO DE LAS SEGURIDADES DE LAS TRANSACCIONES EN LÍNEA EN EL ECUADOR, AÑO 2022 AUTORES: AYME PAREDES DARWIN ARIEL SANDA CHIMBO RONALD EDUARDO DIRECTOR: ING. DARWIN CARRIÓN GUARANDA – ECUADOR 2022
TEMA DEL PROYECTO DE INVESTIGACIÓN ESTUDIO DE LAS SEGURIDADES DE LAS TRANSACCIONES EN LÍNEA EN EL ECUADOR, AÑO 2022
II AGRADECIMIENTO Agradezco a Dios por cada mañana darme las fuerzas para seguir adelante con mi carrera, por darme sabiduría para tomar buenas decisiones en el transcurso de mi vida universitaria, así mismo a mis padres por el amor desinteresado que han tenido conmigo, por el apoyo económico, sus valores y principios que los he llevado desde siempre y para siempre. A todos mis seres queridos por su ayuda y por confiar en mí. A mis profesores que con su comprensión supieron enseñarme la teoría para poderla aplicar en la práctica. Y especialmente a mi tutor Darwin Carrion quién supo servirme de guía para elaborar mi trabajo de titulación, por toda la paciencia brindada a lo largo de toda la tutoría del trabajo. Ayme Paredes Darwin Ariel A mi Dios todopoderoso que me brinda vida, salud, sabiduría y me continúa conduciendo por senderos de rectitud. A mi familia por apoyarme en todo momento ya que son la motivación que me impulsa a ser mejor cada día y a alcanzar los objetivos propuestos. Al Ing. Darwin Carrión, mi tutor en este trabajo de investigación, por su guía y entrega durante el desarrollo de este proceso. Finalmente, mi agradecimiento total a la Universidad Estatal de Bolívar en especial al personal y distinguidas autoridades de la Facultad de Ciencias Administrativas Gestión Empresarial e Informática. Y a todos quienes de alguna u otra manera hicieron posible este logro. Ronald Eduardo Sanda Chimbo
III DEDICATORIA A mi Dios en todo instante, su compañía y misericordia me han permitido llegar a este anhelado momento. Con él todo y sin él nada. Al pilar de mi vida que es mi familia, a mis padres Marco Ayme y Miriam Paredes, que a pesar de lo duro que fue para ellos el proporcionarme la educación siempre mantuvieron la meta de que cumpla mis sueños, que me enseñen que las
Escribe aquí para buscar
In 3 days
17/11/2022

ESTATAL DE BOLIVAR
LA DE SITEMAS
COORDINACIÓN


UNIVERSIDAD ESTATAL DE BOLIVAR
ESCUELA DE SITEMAS
COORDINACIÓN