



Pontificia Universidad
Católica del Ecuador

FACULTAD DE INGENIERÍA

CARRERA DE SISTEMAS

**TRABAJO DE TITULACION PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERO
EN SISTEMAS Y COMPUTACIÓN**

**Tema: Factibilidad Técnica para Desarrollo de una Pasarela de Pagos para
Proveedores en el Ecuador**

AUTOR: JUAN CARLOS GARCÍA SILVA

QUITO, 2020 – ABRIL

Agradecimiento

Agradezco a Dios por las fuerzas que me ha brindado para poder cumplir todo lo que me he propuesto tanto en lo personal como profesional.

Infinitas gracias a mi madre a mis abuelos que no ser por su apoyo no estuviera donde me encuentro en este momento.

Gracias a mis padrinos por confiar en mí, por apoyarme en todo lo que he necesitado, por brindarme su sabiduría para seguir adelante en cada momento adverso que se me ha presentado.

Gracias a mis tíos y a todos ellos por inculcarme sus valores y principios que me hacen ser la persona que soy en este momento.

Agradezco a mis docentes en la Facultad de Ingeniería de la Pontificia Universidad Católica del Ecuador, por haber impartido sus conocimientos a lo largo de mis estudios en esta carrera tan bonita, en especial, al Ing. Javier Córdor como director de mi proyecto quien me ha guiado con su gran conocimiento en la realización del mismo.

Dedicatoria

El presente trabajo se lo dedico principalmente a mi madre, a mis abuelos y mis tíos que han sabido guiarme a lo largo de este camino para alcanzar una meta más en mi vida.

Ellos con su amor incondicional y su apoyo me han hecho llegar hasta culminar esta etapa, todos han aportado su granito de arena para convertirme en una gran persona.

Está dedicado a mi novia que ha sabido ser incondicional en todo momento especialmente con sus palabras de aliento para poder culminar el presente trabajo.

Finalmente, todos mis amigos y amigas que han mostrado su apoyo y han sabido extender su mano de ayuda en los momentos más difíciles a lo largo de mi carrera.

Gracias a todos.

Contenidos

1. Capítulo 1: Marco Teórico	5
1.1. Marco Financiero	5
1.2. Marco Tecnológico	6
1.3. Pasarela de pago	11
1.3.1. Estructura	11
1.3.2. Funcionamiento	11
1.3.3. Políticas y estándares	12
2. Capítulo 2: Situación Actual de Pasarelas de Pago	14
2.1. Historia	14
2.2. Billeteras Electrónicas (E-Wallets)	14
2.3. PayPal	15
2.4. Stripe	16
2.5. KUSHKI Pagos	16
2.6. PAYMENTEZ	17
2.7. PlacetoPlay	17
3. Capítulo 3: Diseño Conceptual de Pasarela de Pagos	18
3.1. Diagrama para compra en línea	18
3.2. Definición del Switch Transaccional para Pasarela de Pagos	19
4. Capítulo 4: Propuesta Técnica de Pasarela de Pagos	22
4.1. Información	22
4.2. Transparencia	22
4.3. Privacidad	22
4.4. Marco legal y regulatorio	22
4.5. Seguridad	22
4.6. Riesgos	26
4.7. Políticas y estándares	29
4.8. Diagrama de casos de uso	31
4.9. Diagrama de clases	32
5. Conclusiones y Recomendaciones	33

5.1. Conclusiones.....	33
5.2. Recomendaciones	34
6. Bibliografía	35

1. Capítulo 1: Marco Teórico

Este capítulo muestra los conceptos que se utilizan para la máxima comprensión del presente estudio de factibilidad.

Estos conceptos hacen referencia a herramientas tanto tecnológicas como financieras que nos permitirán desarrollar este estudio.

1.1. Marco Financiero

Para el desarrollo de este estudio se deben analizar los siguientes términos financieros.

“Banca Electrónica: Tipo de banca que presta sus servicios a sus clientes a través de diferentes tecnologías de comunicaciones, como el internet o líneas telefónicas (banca telefónica). Es también conocida como banca a domicilio.

Comisión: Retribución dada a la persona (comisionista) que actúa como intermediario, realizando una transacción a nombre de otro a título oneroso. **Comisión Flat:** Aquella comisión que se entiende como cantidad única o fija y de una sola vez.

Costo: Precio pagado o solicitado para la adquisición de bienes o servicios. Precio o gasto de elaboración de un producto.

Costo por consumo en establecimientos del exterior: Tarifa que paga el cliente por cancelar los consumos (compras) realizados en establecimientos en el exterior través de la tarjeta de débito.

Costo por consumo en establecimientos nacionales: Tarifa que paga el cliente por cancelar los consumos (compras) realizados en establecimientos nacionales a través de la tarjeta de débito.

Costo por créditos y débitos: Tarifas que paga el cliente por acceder a diversos servicios. Por ejemplo, se realiza el pago de los servicios básicos a través de una cuenta de ahorros o cuenta corriente, se debitará dicho valor de su cuenta, por otro lado, si le depositan el sueldo se acreditará en su cuenta; en ambos casos la institución financiera le cobrará un costo por dichas operaciones.

Institución Financiera: Sociedad que interviene en los mercados financieros, cuya actividad consiste en captar fondos del público e invertirlos en activos financieros.

Instituciones financieras públicas: Instituciones financieras privadas: los bancos, las sociedades financieras o corporaciones de inversión y desarrollo, las asociaciones mutualistas de ahorro y crédito para la vivienda y las cooperativas de ahorro y crédito que son intermediarios financieros del público.

Intermediario: *Persona física o jurídica que actúa como enlace entre dos o más partes que desean realizar una compraventa u otro tipo de operación.*

Intermediario Financiero: Intermediario que actúa de manera habitual en el mercado financiero, receptando recursos través de depósitos o cualquier otra forma de captación, con el objeto de utilizar los recursos así obtenidos, total o parcialmente, en operaciones de crédito e inversión. Ejemplo: los bancos y sociedades financieras, cooperativas y mutualistas.

Tarjeta de crédito: *Es un documento que permite a su titular – o beneficiario de la tarjeta – adquirir bienes o servicios en establecimientos afiliados al sistema, difiriendo su pago o a crédito. Estos créditos pueden o no incluir intereses. Su uso incluye algunas tarifas, costos de emisión, costo de estado de cuenta, intereses y comisiones. Las tarjetas de crédito son intransferibles y deben emitirse a nombre de su titular. El pago mensual puede efectuarse del monto total de la obligación o del monto mínimo; sin embargo; el realizar solo un abono mínimo implica el pago de intereses.*

Tarjeta de débito: *Es una tarjeta de plástico con banda magnética, usada para retirar dinero de un cajero automático y también para pagar los consumos (compras) realizados en locales en donde tengan un terminal lector de tarjetas. Se diferencia de la tarjeta de crédito en que el dinero que se usa nunca es tomado en crédito sino del que se dispone de la cuenta de ahorros o cuenta corriente (débito).*

Utilidad: *Beneficio o ganancia. Excedente de ingresos, productos, equivalente a la diferencia entre ventas totales y costos correspondientes.” (Super Intendencia de Bancos, 2020).*

1.2.Marco Tecnológico

Para el entendimiento de este estudio se debe listar los siguientes términos tecnológicos.

Criptografía

Como lo menciona (Solis, Roque, & Morilla, 2013). *“La criptografía es el arte o ciencia de cifrar y descifrar información mediante técnicas especiales y es empleada frecuentemente para permitir un intercambio de mensajes que sólo puedan ser leídos por personas a las que van dirigidos y que poseen los medios para descifrarlos. Las aplicaciones fundamentales de la criptografía son el cifrado y la firma electrónica. Ambas aplicaciones son el núcleo del comercio electrónico y de cualquier transacción segura que se realice por Internet.*

Para mantener la información a salvo de todos, a excepción del emisor y el receptor legales de la misma y que permiten garantizar que el pago se ha realizado, se usan las técnicas de cifrado. No solamente van a ser utilizados para cifrar los datos, si no que van a permitir una explotación de sus posibilidades más amplia.

Las técnicas de cifrado tratan de asegurar que:

- *Sólo el receptor debe ser capaz de acceder a los datos en claro (confidencialidad).*
- *Nadie ha podido añadir, quitar o cambiar los datos originales del mensaje, o los que puedan acompañarlo (integridad).*
- *El mensaje o los datos provienen de quien dice ser (autenticación).*

Para lograrlo se emplean los algoritmos de cifrado simétricos y asimétricos. Para descifrar los mensajes mediante los algoritmos simétricos, el receptor tiene que aplicar sobre el mensaje cifrado la misma clave que empleó el emisor para cifrar el mensaje original. Los algoritmos simétricos conocidos son: DES, Triple DES, IDEA, RC2, RC4 y RC5. Los algoritmos asimétricos (o de clave pública como también se conocen) se basan en el uso de dos claves diferentes. Una clave puede descifrar lo que la otra ha cifrado. Las claves pública y privada tienen características matemáticas especiales, de tal forma que se generan siempre a la vez y por parejas. Ejemplos de algoritmos asimétricos: Diffie-Hellman, El Gamal, RSA.”

La criptografía es la antesala que nos permite ahora tener protocolos de seguridad para todos los movimientos transaccionales en línea tanto desde las financieras hasta el consumidor final.

Framework

En general, con el término framework, nos estamos refiriendo a una estructura software compuesta de componentes personalizables e intercambiables para el desarrollo de una aplicación. En otras palabras, un framework se puede considerar como una aplicación genérica incompleta y configurable a la que podemos añadirle las últimas piezas para construir una aplicación concreta. Es utilizado en varios ambientes y ámbitos en el desarrollo de sistemas siendo este un ambiente de trabajo con una estructura definida con distintos lenguajes de programación que permiten la creación de todo tipo de software desde aplicaciones móviles hasta aplicaciones en la web. (Gutierrez, 2006)

El objetivo principal en este estudio de la utilización de un framework es el diseño de un prototipo automatizando procesos con muchas ventajas permitiendo así elaborar una propuesta técnica bien definida.

Protocolos

“Un protocolo es un acuerdo entre un aparato y otro para cómo se van a hablar. El protocolo más importante, el básico, es el IP, que es el acuerdo de como hacen los paquetes, como es un paquete, como se pone la dirección, la cabecera del paquete, como se corrigen los errores, ese es el IP.

El protocolo de transmisión de a través de Internet es una combinación del IP (como es el paquete) y TCP (como se transmite).

El protocolo IP solo es el responsable de que el paquete(datagrama) este bien construido, mientras que el protocolo TCP/IP es el responsable de que el paquete llegue a su destino a través de Internet. TCP es el protocolo de transporte. Ambos se utilizan conjuntamente y los dispositivos se configuran para soportarlos si se va a acceder a Internet, a través de cualquiera de las modalidades disponibles.” (Huidrobo, 2017)

SSL

El protocolo Secure Socket Layer (SSL) facilita la autenticación y privacidad de la información en internet mediante el uso de la criptografía. Sólo el servidor es autenticado (es decir, se garantiza su identidad) mientras que el cliente se mantiene sin autenticar; la autenticación mutua requiere un despliegue de infraestructura de claves públicas para los clientes. El SSL se ejecuta en una capa entre los protocolos de aplicación como el Hypertext Transfer Protocol (HTTP). Proporciona sus servicios de seguridad utilizando la criptografía de llave pública y privada. Para el intercambio de los datos entre el servidor y el cliente, utiliza algoritmos de cifrado simétrico. Para la autenticación, usa el algoritmo de cifrado de clave pública (RSA). (Solis, Roque, & Morilla, 2013)

HTTP/HTTPS

El protocolo HTTPS es la versión segura de HTTP. Fue desarrollado por Enterprise Integration Technologies (EIT). Permite el cifrado y autenticación digital igual que SSL. La diferencia está, en que HTTPS es un protocolo de nivel de aplicación, es decir, que extiende el protocolo HTTP por debajo. HTTPS es usado para asegurar páginas World Wide Web para aplicaciones de comercio electrónico, utilizando certificados de clave pública para verificar la identidad de los participantes. (Solis, Roque, & Morilla, 2013)

UML

Lenguaje Unificado de Modelado “UML”, es el lenguaje de modelado de sistemas de software más conocido y utilizado en la actualidad. Se lo puede definir como un lenguaje gráfico para visualizar, especificar, construir y documentar un sistema. (Cevallos , 2015)

UML ofrece un estándar para describir un “plano” del sistema (modelo), incluyendo aspectos conceptuales tales como procesos de negocio, funciones del sistema, y aspectos concretos como expresiones de lenguajes de programación, esquemas de bases de datos y compuestos reciclados. (Cevallos , 2015)

Diagramas de Casos de Uso

Los diagramas de caso de uso modelan la funcionalidad del sistema usando actores y casos de uso. Los casos de uso son servicios o funciones provistas por el sistema para sus usuarios. (Cevallos , 2015)

Diagramas de Clases

Este tipo de diagrama de UML se utiliza para representar la estructura estática del programa, las clases se representan mediante un rectángulo. En el formato más simple, el rectángulo puede incluir sólo el nombre de la clase, pero también puede incluir atributos y métodos. Los atributos son lo que la clase conoce sobre las características de los objetos, y los métodos (también llamados operaciones) son lo que la clase sabe acerca de cómo hacer las cosas. Los métodos son pequeñas secciones de código que trabajan con los atributos. (Cevallos , 2015)

E-Wallet

Una cartera digital se refiere a un dispositivo electrónico que permite a una persona hacer transacciones de comercio electrónico. Esto puede incluir comprar artículos en línea con una computadora o usar un teléfono inteligente para comprar algo en una tienda. Cada vez más, carteras digitales se están haciendo no sólo para las transacciones financieras básicas, sino también para autenticar las credenciales del titular. Por ejemplo, una cartera digital podría potencialmente verificar la edad del comprador a la tienda mientras compraba alcohol. Es útil abordar el término "cartera digital" no como una tecnología singular, sino como tres partes principales: el sistema y la aplicación y el dispositivo. La cuenta bancaria de un individuo también se puede vincular a la cartera digital. También pueden tener su licencia de conducir, tarjeta de salud, tarjeta de lealtad y otros documentos de identificación almacenados en el teléfono. Las credenciales se pueden pasar al terminal de un comerciante de forma inalámbrica a través de la comunicación de campo cercano. Ciertas fuentes están especulando que estas "carteras digitales" del teléfono elegante substituirán eventual las carteras físicas. (Educalingo, 2020)

E-commerce

El e-commerce, ecommerce o comercio electrónico es simplemente emplear internet como medio para la compraventa de servicios, bienes o productos. Es decir, el comercio de forma online empleando internet como medio de comunicación. (e-commerce-que-es, 2015)

Portal Web

El portal web es una página de comercio electrónico con la finalidad de vender productos o servicios con varios métodos de pagos para el cliente final.

Herramienta de modelado

El UML, o Lenguaje de Modelado Unificado, abstrae y visualiza sistemas de la programación orientada a objetos. El lenguaje de modelado es, por lo tanto, una herramienta práctica para los desarrolladores de programas y sistemas. Por un lado, permite crear fotocalcos claros para proyectos de software, y por otro, presentar sistemas de programación complejos de forma comprensible para las personas que no están familiarizadas con la temática. Por ejemplo, si deseas presentar un proyecto de software al responsable de marketing, por medio de un

diagrama UML puedes ofrecer una visión general de las características más importantes de la aplicación. (Digital Guide Ionos, 2019).

La herramienta de modelado usada en este trabajo de titulación será Edraw Max.

Edraw Max

“Un software de diagramación todo incluido para el sistema Windows que es capaz de más de 260 tipos de dibujos, incluidos diagramas de flujo, mapas mentales, organigramas, infografías, planos de planta, diagramas de red, diagramas de Gantt, esquemas eléctricos ... y eso es solo el comienzo.

Más de 260 tipos de diagramas lo ayudan a analizar datos fácilmente y presentar información de manera agradable. Haga que el contenido complejo y las estadísticas sean comprensibles de un vistazo. Convierta informes tediosos en infografías atractivas. Al vincular formas a datos, insertar hipervínculos y archivos adjuntos, este software de diagrama de Linux aumentará enormemente la comunicación”. (Cnet, 2020).

Switch Transaccional

“El Switch Transaccional es un middleware transaccional que permite el funcionamiento de B2B en nuestro medio pues es capaz de hacer transacciones que reflejan los resultados, obteniendo en las transacciones los depósitos de datos de las empresas participantes.

El Switch Transaccional utiliza “Programación Remota”, lo que permite acceder mediante el protocolo TCP a aplicaciones que a su vez se conectan a sus respectivos servidores de base de datos.

El Switch Transaccional maneja el concepto de servicios, que son transacciones configuradas por cualquier empresa que desee brindar un servicio a otras empresas que deseen suscribirse al mismo. Por esto las empresas participantes tendrán dos roles claramente definidos dentro del Switch Transaccional, empresa que brinda servicios y empresa que se suscribe a un servicio.

Un servicio consta de una o más operaciones (Propiedad que brinda la empresa que lo ofrece al momento del registro), cada operación es una transacción realizada a la base de datos de sí misma, pudiendo consultar información o brindar la posibilidad de permitir insertar o actualizar datos.

Una suscripción es también un servicio, pero este es configurado en base al servicio elegido mediante este proceso, en esta etapa también intervienen el registro de las operaciones que son punto principal para que los resultados obtenidos sean los correctos.

Cada empresa tendrá la responsabilidad en el momento de la configuración de registrar sus estructuras de datos en una operación elegida, teniendo como diferencia que la empresa que se suscriba a un servicio tendrá la responsabilidad de asociar sus estructuras de datos con aquellas pertenecientes a la empresa a la cual se suscribió”. (Béjar, Luzuriaga, & Echeverría, 2006)

1.3.Pasarela de pago

“Una pasarela de pagos es una página web que representa un servicio intermediario entre una página de comercio electrónico y un banco cuando se ejecutan transacciones bancarias online. Se integran a la tienda virtual y almacenan información del banco que maneja las cuentas de compradores y vendedores. En el pago con tarjeta, la pasarela de pagos valida la veracidad de la tarjeta y organiza la transferencia del dinero de la cuenta del comprador a la cuenta del vendedor.

Son llamadas terminal de punto de venta (TPV) virtual, pero no son realmente terminales de punto de venta porque estas últimas sí pertenecen al banco y el vendedor debe tener una cuenta en el banco en donde esté implementado el TPV virtual. Para el proceso de pago o transferencias bancarias es necesaria la utilización de tarjetas de crédito o débito como medios electrónicos de pago.” (Solis, Roque, & Morilla, 2013).

1.3.1. Estructura

La estructura de una pasarela de pagos consta de los siguientes elementos:

Base de datos, página Web, conexión con comercio electrónico, conexión con entidad financiera.

1.3.2. Funcionamiento.

El funcionamiento de una pasarela de pagos consta del siguiente proceso entre la entidad bancaria, cliente y tienda.



Figura 1 – 01 ¿Cómo funciona una Pasarela de pagos online? (TPVVIRTUAL, 2019)

Como se menciona en la figura 1 – 01 los pasos para el funcionamiento de una pasarela de pagos es la siguiente:

Productos o servicios, tienda en línea, pasarela de pago, banco, tarjeta de crédito o débito, banco al cual pertenece la tarjeta, protocolo de seguridad para fraudes, transacción realizada o rechazada, transferencia a banco.

1.3.3. Políticas y estándares.

De acuerdo al Manual de Buenas Prácticas de las Pasarelas de Pago en Colombia se señalan las siguientes políticas y estándares para una pasarela de pago.

“Garantizar que los operadores tengan un soporte disponible y accesible, si enfrentan algún problema.

El operador tiene que identificar el tipo de soporte que se ofrecerá (correo electrónico, centro de llamadas, etc.), la capacidad de respuesta del soporte ofrecido y el costo involucrado en el mismo;

Establecer políticas claras para la vinculación de los comercios, las cuales deberán atender lo desarrollado por la CE 8 de 2018 y especialmente la firma y/o aceptación de los términos y condiciones de la Pasarela.

Definir una política de prevención de lavado de activos y financiación del terrorismo que precise los lineamientos, controles y acciones necesarios para protegerse del riesgo de LA/FT¹, atendiendo al ambiente no presencial en el que operan las pasarelas de pago; para esto, las pasarelas deberán establecer procesos de conocimiento al cliente expeditos y con un mínimo de documentación que permita el cotejo de identidad y de origen de sus recursos, preferiblemente a través de mecanismos electrónicos tales como consultas en fuentes públicas o bureaus de crédito.

Desarrollar procesos para identificar, medir, controlar y monitorear el riesgo de LA/FT;

Evaluar el cumplimiento técnico y la efectividad de los estándares internacionales en materia de gestión de riesgos de LA/FT.

Cumplir con los estándares de debida diligencia, implementando mecanismos para lograr una debida diligencia en el conocimiento del cliente, sin recurrir a los mecanismos tradicionales (entrevista, formulario);

Definir una política de sanciones por el incumplimiento o violación a las políticas de prevención de LA/FT;

Desarrollar una metodología para la detección de operaciones inusuales, intentadas y sospechosas, y el oportuno y eficiente reporte de estas últimas a las autoridades competentes;

¹ LA/FT: Hace referencia al Lavado de Activos y al Financiamiento del Terrorismo.

Los operadores de pasarelas de pago deben aplicar estándares mínimos para la adecuada atención y manejo del fraude.

Generar un canal de comunicación para facilitar el canje de información relevante entre la pasarela y las entidades, en desarrollo de la actividad de intercambio de información;

Notificar al operador, cuando se bloquea una transacción en un sistema antifraude por considerarla de alto riesgo o sospechosa, las razones por las que se niega la transacción.

Estructurar el modelo gerencial, estratégico y operativo del Procesador de Información de Fraude de tal manera que se asegure su puesta en marcha y su seguimiento a través de indicadores de gestión y un esquema de mejoramiento de oportunidades;

Registrar la operación de anulación en el sistema de información de las redes para que posteriormente las entidades sean notificadas y apliquen los cambios respectivos en el estado de cuenta del cliente;

Diseñar dentro de la relación contractual con el comerciante, un mecanismo de confirmación de información para indagar detalles de la transacción en disputa antes de gestionar un contra cargo;

Definir dentro de la relación contractual con el comerciante, un tiempo límite en el análisis del contra cargos, reversiones y anulaciones para que el cliente tenga una respuesta clara sobre su reclamación;

Establecer dentro de la relación contractual con el comerciante, un protocolo de comunicación en el proceso de contra cargos para que se dé un flujo de comunicación adecuado y expedito de tal manera que el cliente tenga claridad sobre a quién dirigirse y la evolución de su caso entre otros aspectos.” (Rincón, 2018).

Las pasarelas de pago se emplean en el mundo del comercio electrónico, al ser una página web estas crean el nexo entre la entidad bancaria, la tienda en línea y el cliente final para poder realizar los pagos con tarjetas de crédito y débito.

2. Capítulo 2: Situación Actual de Pasarelas de Pago.

En este capítulo se presentará cual es la situación actual de las pasarelas de pagos adicionalmente vamos a poder observar que en el Ecuador operan varias pasarelas de pagos las cuales son contratadas por las páginas de comercio electrónico.

2.1.Historia

Con el paso de los años podemos evidenciar la evolución de las formas de pagar los productos o servicios empezando por el trueque en el siglo VII a.C. cuando se intercambiaba entre víveres y especias por otros productos o piedras preciosas.

En segunda instancia en el siglo XVIII d.C. llegó el billete que se lo utiliza hasta la actualidad siendo este aún el método más común, pero con el tiempo se ha venido mermando su uso por distintos motivos.

La creación de la tarjeta de crédito como medio de pago no fue especialmente emitida por una entidad bancaria como lo afirma (Perez, 2019) “La era ‘moderna’ en los medios de pago trajo las tarjetas de crédito: La primera tarjeta de crédito, curiosamente, no fue emitida por un banco. En 1914 la Western Union creó una tarjeta de fidelización para sus clientes más selectos, que permitía además el acceso a crédito”.

Ya enfocándonos dentro de los medios de pagos electrónicos y siendo como tal una pasarela de pagos en 1998 PayPal aparece siendo esta la más popular y versátil.

A continuación, se listan las pasarelas de pagos más utilizadas en nuestro país con sus respectivas características y ventajas dentro del comercio electrónico.

2.2.Billeteras Electrónicas (E-Wallets)

Las billeteras electrónicas han revolucionado la forma de pago por los convenios que han logrado realizar las grandes empresas como Apple, Google y Amazon. A continuación, se describe las 3 billeteras electrónicas más importantes.

Apple Pay

Como lo asevera (Apple, 2019) “*Apple Pay permite realizar transacciones de forma rápida, segura y privada en tiendas, en aplicaciones y en la Web. También puedes enviar dinero a amigos y familiares, así como recibirlo, mediante Apple Pay en Mensajes (disponible solo EE. UU.). Además, con las tarjetas de fidelización sin contacto en Wallet, puedes conseguir y canjear premios al pagar con Apple Pay. Apple Pay es una forma más sencilla y segura de pagar que las tarjetas de*

crédito, débito o prepago físicas, ya que se ha diseñado teniendo en cuenta tu seguridad y privacidad.”

Google Pay

Google Pay es una plataforma para realizar pagos online y mediante tu móvil a través de tu cuenta de Google, muy parecidas a otras alternativas como Apple Pay. La herramienta nació en febrero de 2018 como una unión entre Android Pay y Google Wallet, aunque realmente es más una sucesora de la primera, siendo su enfoque principal el de permitirte hacer pagos con el móvil. (Xataka, 2019)

Amazon Pay

Amazon Pay es un nuevo servicio de intermediación a la hora de realizar pagos en una web. Es algo muy parecido a PayPal, y te ayuda cuando quieres hacer una compra en una web sin facilitar tus datos personales. En las tiendas online donde esté habilitado, será suficiente con pulsar el botón de Amazon Pay e identificarte con tu cuenta de Amazon para realizar el pago. (Xakata, 2017)

2.3. PayPal



“En 1998 Ken Howey y Max Levchin fundan la empresa estadounidense Paypal, llamada en aquel entonces Confinity, que es el resultado de la mezcla de dos palabras: Confidence e Infinity. La principal función era la transferencia de dinero únicamente por un PDA (Personal Digital Assistant o Ayudante personal digital), pero con el tiempo la web fue ganando terreno y se necesitó de otra plataforma para cubrir sus necesidades.


Posteriormente, se unen a la compañía tres personajes que le dieron un nuevo giro a la empresa: Elon Musk, Peter Thiel y Luke Nosek. Tras su integración, Confinity cambia su nombre al actual Paypal, que su objetivo principal fue el de proveer servicios de pago por internet con el uso de tarjeta.

Con el paso del tiempo su éxito seguía viento en popa, se mezclaron a grandes empresas como lo es MasterCard, que desarrolló un servicio que permitía a los clientes realizar pagos en sitios web que no aceptaban PayPal. Esto generó grandes beneficios económicos, logrando el primer trimestre del 2009 16 millones de transacciones.

De acuerdo al Portal Reuters, en el año 2015 Paypal alcanzó un valor de 52,000 millones de dólares. Según diversos analistas “es el gigante entre los proveedores de servicios de pagos digitales independientes con más de 160 millones de cuentas activas, escala global y reconocimiento de marca”. Sin duda, se ha vuelto un referente de esta época, la mayoría de las personas pueden distinguir su logo y lo ven en un sinfín de sitios. Paypal no sólo llegó a facilitar el


sistema de pagos, sino que lo revolucionó, creando un antes y un después en la historia de la humanidad.” (Paypal, una historia de éxito, 2017).

2.4.Stripe

 Stripe es otro de los proveedores de pago de servicio completo más populares, lo que significa que incluye su pasarela de pago y su cuenta de comerciante, y es el medio para crear tu propio sistema de pago personalizado. Las ventajas que más valoran sus usuarios son, que sea una plataforma intuitiva, que sea una opción de pago recurrente, que ofrezca informes de ventas en vivo y cuente con excelentes tarifas para tarjetas de la UE. Los pagos han evolucionado con la llegada de las nuevas tecnologías, pero su esencia permanece sin cambios: los bienes y servicios se intercambian por el pago de un valor acordado mutuamente entre el comprador y el vendedor. En la era digital contamos con una clara diversidad de ecosistemas de pagos que surge naturalmente de nuestras respectivas diferencias culturales, políticas y económicas. (Quelle, 2020)

Para más información sobre esta pasarela de pagos su web es: <https://stripe.com/es>

2.5.KUSHKI Pagos

 De acuerdo a (Hernandez, 2019) *“Kushki es una pasarela fundada por Sebastián Castro (Ecuador), que combina una solución completa de pagos, con tecnología segura, ágil y sencilla, con el fin de aumentar la conversión de compradores. Esta herramienta está conformada por ejecutivos que tienen más de 20 años en el mercado y cuentan con sede en Brooklyn, Boston, Bogotá y claro está, Quito.*

Esta plataforma, ofrece una tecnología moderna que permite integrar fácilmente distintas formas de pago, combinado con dinamismo, lo que le ha permitido ubicarse en el top de pasarelas en el Ecuador en menos de un año funcionando en el país.

En el Ecuador, Kushki pudo abrir débito con todas las entidades bancarias, ofreciendo de este modo, una mejor experiencia de uso a los usuarios de esta plataforma. Este medio también ofrece un procesamiento de pagos multicanal en tiempo real e integrado a redes sociales para el consumidor móvil y social de hoy día. En estos tiempos modernos, contar con una plataforma de pago integrada y convergente que abarque los canales de tiendas físicas, e-commerce y m-commerce, es muy importante para impulsar el crecimiento en un mercado cada vez más competitivo.

La ventaja estratégica que ofrece Kushki, es convertirse en un socio tecnológico de todos sus clientes, de este modo, redefine el concepto actual que se tiene como proveedor de plataformas de pagos; Asimismo, al empezar a utilizar este servicio, sin importar la cantidad de canales de

venta de un cliente, se ofrece atención de migración digital, con el fin de apoyar a los equipos internos a que se amplíe la transaccionalidad digital, paralelamente al tiempo que elimina el elevado costo del sistema de transacciones de dinero en efectivo. Actualmente en Facturero Móvil la utilizamos para que nuestros clientes realicen sus recargas.”

2.6.PAYMENTEZ



Es una plataforma de pagos en línea que permite procesar pagos locales de sitios de comercio electrónico en el Ecuador. Paymentez también ofrece una excelente experiencia de compra para los clientes, gracias a su sencillez y a sus procesos estructurados. Este medio de pagos se caracteriza por tener una estructura sólida y al mismo tiempo, flexible. (Hernandez, 2019)

Asimismo, se encuentran enlazados con adquirientes locales de tarjetas de crédito por lo que, permiten realizar pagos con tarjetas de crédito ya sea de forma rotativa o diferida, también permite pagos con débitos bancarios, tarjetas prepago y se espera que brinden la opción de transferencias bancarias. (Hernandez, 2019)

Paymentez tiene más de diez años en el mercado, iniciaron procesando pagos en Colombia para juegos en línea de computadoras, así como también de sitios web, aplicaciones móviles, hasta llegar a lo que son ahora: una plataforma integral de pagos en línea. Así pues, cuentan con más de cinco millones de clientes en distintos países además de Ecuador, como México, Panamá, Venezuela, Colombia, Brasil, Argentina y Chile, con una cifra promedio de sesenta mil transacciones al día. (Hernandez, 2019)

2.7.PlacetoPlay



Este botón de pagos, ofrece acompañar a sus clientes en todo el proceso de la transacción: Antes: En este paso, se encargan de autenticar, validar y brindar soluciones técnicas. Durante (Pago): Es el proceso encargado de verificar, clasificar y filtrar los pagos. Después: Procesan, concilian y almacenan todas las transacciones. (Hernandez, 2019)

En cuanto al dinero, se puede recibir directamente en la cuenta bancaria del comerciante o puede llegar a la plataforma de PlacetoPlay, todo depende de los requerimientos del comerciante. PlacetoPlay, tiene más de 15 años en el mercado, principalmente en Colombia, y su objetivo empresarial es tener las herramientas necesarias para respaldar el proceso transaccional de cualquier comercio, en cualquier segmento económico. (Hernandez, 2019)

Una de las ventajas, es que en sus valores está ser una plataforma de transacciones y hace dos años llegó al Ecuador, contribuyendo a la expansión y crecimiento del e-commerce en Ecuador. Web: <https://www.placetopay.ec>. (Hernandez, 2019)

3. Capítulo 3: Diseño Conceptual de Pasarela de Pagos

En este capítulo se realizará el diseño de la interacción entre todos los elementos involucrados en una pasarela de pagos.

3.1. Diagrama para compra en línea

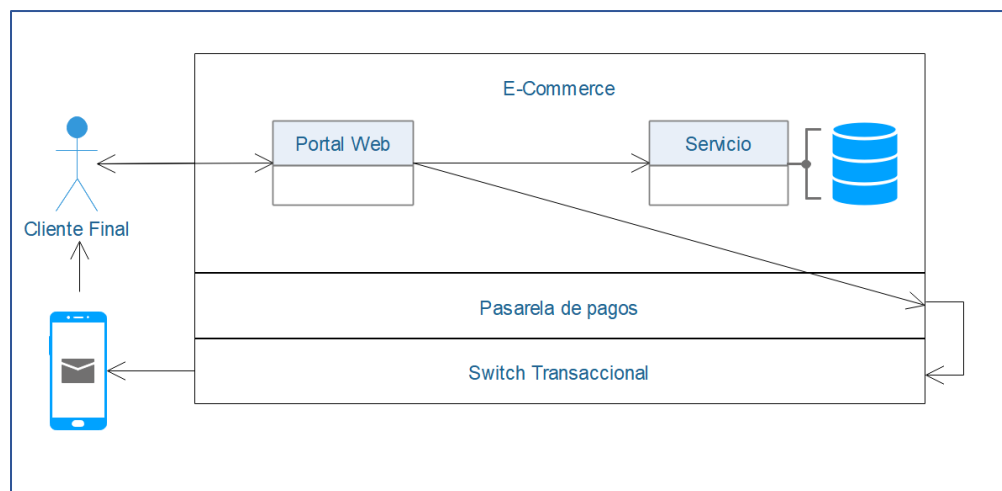


Figura 3 – 01 Interacción e-commerce (García, 2020)

De acuerdo a la figura 3 -01 el sitio de comercio electrónico envía la solicitud a través de un servicio web, este se conecta con una base de datos para registrar las transacciones por sus usuarios.

El portal de comercio electrónico se va a interconectar a la pasarela y este lo hará con el switch transaccional.

El switch transaccional es quien nos va a dar su servicio para poder realizar las transacciones con los distintos medios de pago que tenga afiliado a este, se enviará una notificación al teléfono celular del usuario que es quién autoriza el pago.

Portal Web

El portal web es quien va a consumir el servicio interconectado hacia la pasarela de pagos.

Cliente Final

El cliente final es quién consume los productos o servicios ofertados por el portal de comercio electrónico.

Servicio

El servicio es el que permite la interacción entre el portal web y la base de datos para almacenar las transacciones solicitadas por el cliente final las cuales serán aprobadas o rechazadas después de realizar el proceso de validación por parte del switch transaccional.

Pasarela de Pagos

La pasarela de pagos recibe el mensaje emitido por el portal web para poder procesar la transacción, siendo este un nexo bilateral entre el switch y el portal.

La pasarela de pagos envía la solicitud de proceso de la transacción a través de una URL con un certificado digital y una clave que permite el acceso al switch transaccional.

Switch Transaccional

El switch transaccional recibe la solicitud de la pasarela de pagos con un servicio y provee la seguridad entre la comunicación para que sea un éxito la transacción.

En producción las conexiones se tienen que hacer vía VPN, simplemente son las direcciones IP registradas que consume los servicios interconectados al switch.

Este realiza la aprobación o rechazo de la compra con una notificación de mensaje de texto que autoriza el cliente final.

Existen 2 switch transaccionales en el Ecuador. Estos se manejan tanto en la red privada y pública. La economía popular y solidaria manejan todo el tema de las cooperativas de ahorro y crédito. Su uso es por parte de los habitantes viene en un crecimiento constante dentro de las zonas rurales y cantones del Ecuador.

Dentro de la parte privada el switch de Banred es quien tiene asociado a los bancos y tarjetas de crédito; por la parte pública lo maneja directamente el Banco Central del Ecuador.

3.2. Definición del Switch Transaccional para Pasarela de Pagos

De acuerdo al Switch Transaccional Basado en el Paso de Mensajes XML vamos a observar la visión de las consideraciones que se deben tomar cuando se consume un servicio como pasarela de pagos.

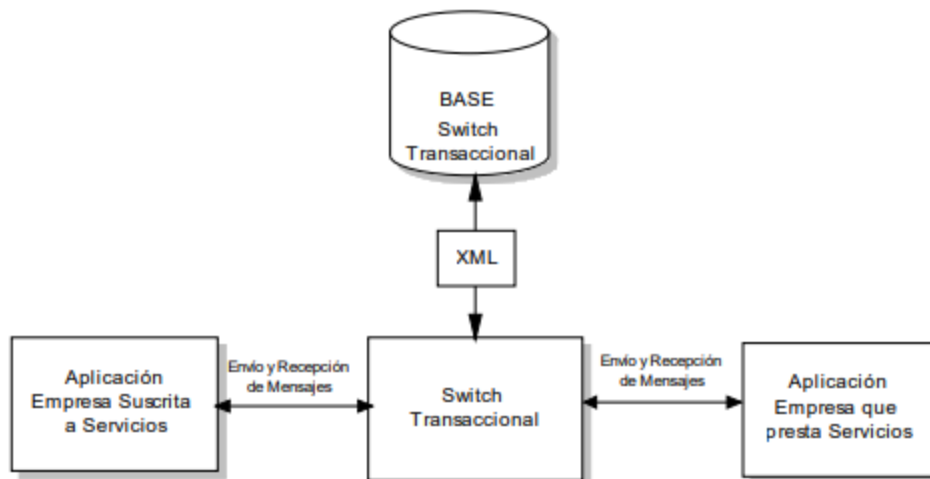


Figura 3 – 02 Arquitectura Switch Transaccional (Béjar, Luzuriaga, & Echeverría, 2006)

“Definición de la arquitectura del Switch Transaccional desde el punto de vista de Empresa que presta servicios

Una empresa que va a brindar un servicio empieza registrando sus datos generales dentro del Switch Transaccional, a continuación, la empresa queda lista para registrar su servicio.

La empresa debe definir el servicio dando al mismo, nombre, descripción, el número de operaciones a utilizar, así como el nombre y funcionalidad de cada operación

La empresa debe configurar cada operación según el orden y funcionalidad dados en el registro del servicio, para esto debe ingresar las estructuras correspondientes de acuerdo al tipo de operación que ingresó.

Según las estructuras de datos ingresadas el Switch Transaccional contará con la sentencia transaccional a ser utilizada en la aplicación de la empresa.

Definición de la arquitectura del Switch Transaccional desde el punto de vista de Empresa que se suscribe a un servicio

La empresa que suscribe un servicio debe registrar sus datos generales para luego pasar a elegir un servicio.

Según el servicio elegido a la empresa observará un resumen del mismo, proporcionándole el nombre, descripción y funcionalidad por operación.

La empresa debe ingresar el tiempo que ejecutan las transacciones.

Se presenta a la empresa las operaciones que constan en el servicio al que se está suscribiendo, por lo que debe configurar sus operaciones en base a éstas.

La empresa debe ingresar las operaciones transaccionales que van a relacionar con el servicio elegido.

Por cada operación a registrar la empresa debe ingresar sus estructuras de datos.

En la configuración presentan los campos que ha ingresado, así como los que corresponden a la operación actual, por lo que debe asociar los campos, siendo responsable de la forma en la cual van a interactuar sus datos con los datos proporcionados por la empresa que brinda el servicio.” (Béjar, Luzuriaga, & Echeverría, 2006; Béjar, Luzuriaga, & Echeverría, 2006).

4. Capítulo 4: Propuesta Técnica de Pasarela de Pagos

En este capítulo se realizará una propuesta técnica para pasarela de pagos tomando en cuenta desde el manejo de la fidelidad de datos, políticas, riesgos y buenas prácticas hasta la interacción de los actores y procesos en las tecnologías de la información para el diseño tecnológico de un software.

4.1. Información

Dentro del comercio electrónico existen operadores para las pasarelas de pagos, ellos manejan grandes cantidades de información que deben ser tratadas con el debido recaudo y siempre comunicar absteniéndose de ocultar al cliente acerca de todas las transacciones que se estén realizando para su tienda.

4.2. Transparencia

El operador debe ser claro y lucido al realizar los procesos que se llevan a cabo en una pasarela de pagos para no generar dudas a los clientes.

4.3. Privacidad

El operador debe tener reserva absoluta acerca de todos los datos de sus clientes, es decir, datos personales, identidades, transacciones, a menos que exista una autorización por parte del cliente dueño de los mismos.

4.4. Marco legal y regulatorio

Los empresarios tanto la pasarela como los clientes deben ajustarse a las leyes que existen para el manejo de comercio electrónico tanto nacional como internacional evitando cometer delitos por la información que se encuentra comprometida en el manejo de transacciones bancarias.

4.5. Seguridad

A continuación, se propone los siguientes lineamientos para la seguridad de una pasarela de pagos.

Del lado del operador de la pasarela de pagos debe tener en cuenta todas las normas de seguridad para los datos que se encuentra manejando basándose en todo momento a los estándares de comercio electrónico.

Seguridad respecto del recurso humano.

“Se recomienda a las pasarelas:

Diseñar una “política marco de recursos humanos” que defina un modelo de gestión de recursos humanos de la pasarela de pago, que permita captar, impulsar y retener el talento humano, haciéndoles partícipes del proyecto y garantizándoles un puesto de trabajo digno y seguro;

Definir programas de formación que favorezcan la mejora y la conservación del capital intelectual y la promoción de los trabajadores dentro de la pasarela de pagos;

Fomentar canales de diálogo y comunicación con los empleados por medio de subcomisiones o comités de trabajadores, encuestas de clima laboral, encuentros con el presidente y altos directivos, reuniones específicas;

Establecer una política de seguridad y salud laboral que tenga como finalidad, lograr un entorno de trabajo seguro y saludable;

Definir un Código Ético que recoja los principios de actuación exigibles a los trabajadores y directivos, cualquiera que sea su nivel jerárquico o funcional;

Establecer procedimientos normalizados para la contratación del personal, y selección de los profesionales, disminuir la tasa de rotación.

Invertir en la capacitación de los profesionales, ofrecer cursos a cargo de un miembro de la empresa o de un curso externo.” (Rincón, 2018)

Seguridad de la información

“En este punto se recomienda a las Pasarelas:

Garantizar que los servidores de la pasarela sean seguros y proporcionen las siguientes tres garantías:

- Autenticidad. Permite tener la certeza de que los datos del pago se están enviando al auténtico servidor de la entidad financiera;*
- Confidencialidad. Asegura que los datos, en el caso de ser capturados por un tercero ajeno a la transacción, no podrán ser empleados ya que viajan cifrados;*
- Integridad. Garantiza que los datos que llegan al servidor del banco no se han alterado por el camino (internet), detectándose a través de los mecanismos de seguridad de TLS cualquier alteración.*

Disponer de un certificado emitido por una Autoridad de Certificación (como Certificado TLS Symantec2), quien analiza exhaustivamente los datos de la entidad solicitante y las normas de seguridad de su infraestructura, para que un servidor sea seguro.

Emplear por parte del operador el protocolo de seguridad TLS (Secure Sockets Layer) cuyo uso principal es cifrar el número de las tarjetas de crédito al realizar cualquier transacción online.

Considérese que el protocolo TLS ofrece servicio de cifrado de datos, autenticación del servidor, integridad de mensajes y, en menor medida, la identificación del cliente para conexiones TCP/IP (protocolo empleado en internet). TLS proporciona un canal electrónico seguro para realizar transacciones entre los servidores (banco, entidad emisora de la tarjeta y tienda online) y los navegadores a través del cual, cifrando los datos de compra, se pueden celebrar transacciones electrónicas con seguridad.

Otro protocolo de seguridad utilizado por los operadores de las pasarelas de pago es el SET (Secure Electronic Transaction), el cual se caracteriza por ser un conjunto de normas de seguridad cuyo fin es asegurar la identidad de las personas que participan en una transacción electrónica, proteger la información que se envía y garantizar que esta no ha sido manipulada en este proceso. Para ello emplean certificados digitales y software de encriptado que lo hacen más complejo de usar y por lo tanto más difícil de implantar que el TLS.

Cumplir los requisitos técnicos en la captura, almacenamiento, procesamiento y transmisión de la información sensible y datos del cliente. Estos requisitos se encuentran enmarcados dentro de seis principios de la Normas PCI₃:

- *Construir y mantener una red segura;*
- *Proteger los datos de las tarjetas;*
- *Mantener un programa de gestión de vulnerabilidades;*
- *Implementar medidas de control de acceso;*
- *Monitorear y probar regularmente las redes;*
- *Mantener una política de seguridad de la información.*

Tener un sistema de copia de seguridad, también conocido como backup. Es una copia de los datos originales que se realiza con el fin de disponer de un sistema de respaldo en caso de pérdida, deterioro o robo de información;

Los soportes en los que se pueden realizar copias de seguridad son variados, el soporte escogido dependerá del sistema de copias que se elija, de la fiabilidad que se necesita y de la inversión económica que se quiera realizar. Los más utilizados son:

- *Unidades USB y discos duros portátiles;*
- *Discos duros de equipos específicos;*
- *Cintas de seguridad;*
- *Soportes ópticos como DVD o CD;*
- *Almacenamiento de copias en la nube.*

Analizar la información de la que se realizará la copia descartando toda la información que carezca de relevancia. Es necesario incluir todos los equipos de la organización;

Definir el número de versiones que se almacenará de cada elemento y su período de conservación, a esta forma de actuar se la conoce como política de copias de seguridad.

Esta política dependerá del tamaño de la organización y del volumen de información que maneje la pasarela de pago;

Realización de pruebas de restauración ya que si las copias realizadas son inaccesibles o se encuentran dañadas un sistema de pruebas resolvería este problema;

Control de los soportes donde se realiza la copia etiquetando y registrando la ubicación de los soportes. También hay que llevar un control de la vida útil del soporte;

Documentar el proceso de realización y restauración de las copias. En caso de utilizar almacenamiento en la nube hay que contar con la posibilidad de no tener conexión a internet además de estar informado en cuanto a las políticas de privacidad y seguridad en caso de almacenar datos sensibles.” (Rincón, 2018)

Seguridad física

“Al respecto se propone:

Monitorear los controles de seguridad, tales como firewalls, IDS/IPS (sistemas de intrusión-detección o de intrusión-prevención), FIM (monitorización de la integridad de archivos), antivirus, controles de acceso, etc., para asegurarse de que funcionan correctamente y según lo previsto;

Garantizar la detección de todas las fallas en los controles de seguridad y solucionarlas oportunamente. Los procesos para responder en caso de fallas en el control de seguridad son los siguientes:

- Restaurar el control de seguridad;*
- Identificar la causa de la falla;*
- Identificar y abordar cualquier problema de seguridad que surja durante la falla del control de seguridad;*
- Implementar la mitigación (como procesos o controles técnicos) para evitar que la causa reaparezca;*
- Reanudar la monitorización del control de seguridad, quizás con una monitorización mejorada durante un tiempo a fin de verificar que el control funcione correctamente.*

Ofrecer al usuario un sistema de respaldo para las funcionalidades mínimas en caso de que la tienda virtual no funcione. Los sistemas de respaldo pueden encontrarse en una empresa externa a la organización o dentro de la misma. Si se encuentra dentro de la organización es conveniente que el sistema de respaldo no comparta ningún tipo de infraestructura con el servidor principal ya que un problema que afecte al servidor principal podría afectar al servidor de respaldo;

Instalar un firewall. Un firewall es una solución de hardware o software que supervisa la actividad de las conexiones externas (principalmente internet) a una red interna de servidores.

Los cortafuegos ayudan a eliminar actividades externas no autorizadas o no deseadas y autoprotegen su red y conexiones de amenazas externas;

Almacenar toda la información confidencial separada de los servidores web, para obtener máxima seguridad de la información. Si por alguna razón es necesario almacenar estos datos, se debe hacer en una base de datos segura y encriptada en un servidor que no esté conectado a internet. Si la información confidencial se almacena en una copia impresa, debe ser examinada a fondo y eliminar la información regularmente.” (Rincón, 2018)

4.6. Riesgos

Para la implementación de una pasarela de pagos se recomienda hacer una evaluación de los riesgos y como se mitigarán los mismos, tanto en tecnologías de la información como a nivel empresarial para poder tener planes de contingencia frente a cualquier eventualidad.

Valoración de los riesgos

“Es necesario, destacar al respecto lo siguiente:

Desarrollar, previo al ingreso oficial de la pasarela al sistema de comercio electrónico, una valoración de riesgo teniendo en cuenta la situación real de seguridad de la información.

Esta valoración de riesgo deberá ser realizada por un tercero que tenga un adecuado conocimiento de seguridad de la información y de las normas PCI DSS e ISO 270014 y conexas. Los aspectos mínimos por observar, analizar y valorar son los siguientes:

- *Seguridad de la información. Este aspecto se valora con dos preguntas frente a la identificación y control de los riesgos de la información en el comercio, y con una pregunta sobre el responsable de la seguridad de la información en el comercio;*
- *Seguridad del recurso humano. Se valora con tres preguntas frente a la responsabilidad y nivel de conciencia de empleados y terceros con la seguridad de la información en el establecimiento;*
- *Seguridad y gestión de los activos. Este aspecto se valora con dos preguntas relacionadas con los activos del establecimiento y su clasificación en función del nivel de criticidad de estos, relacionados con la gestión de la información;*
- *Seguridad en el acceso a la información y a los activos asociados al proceso de información. Se valora este aspecto con tres preguntas sobre los mecanismos existentes para proteger el acceso no autorizado a la información sensible del establecimiento y sus clientes;*
- *Seguridad de las operaciones. Se valora con tres preguntas enfocadas a establecer la manera de proteger la operación del establecimiento frente a riesgos de comprometimiento de información;*

- *Seguridad de las comunicaciones. Se valora con una pregunta que busca identificar el nivel de protección en los esquemas de comunicación digital y electrónica.” (Rincón, 2018).*

Medidas de protección frente a los riesgos.

“Los operadores de pasarelas de pago deben adoptar una serie de medidas de protección específicas contra los tipos de fraude expuestos anteriormente, toda vez que al ser los responsables del servicio que prestan, es necesario que implementen todos los mecanismos de seguridad posibles que detecten y eviten el fraude y los ataques de ciberdelincuentes facilitando, además, herramientas a sus usuarios que mantengan su seguridad.

Para que las pasarelas de pago funcionen de manera correcta, es necesario adoptar las medidas de seguridad que garanticen un nivel aceptable de seguridad tanto para el operador como para el usuario. Estas son algunas de las medidas de seguridad que deben ser adoptadas por los operadores de las pasarelas de pago:

Los operadores de las pasarelas de pago deben disponer de un certificado TLS o TLS que le permita identificar su sitio web de forma inequívoca, y que garantice que la información que se transmite entre el navegador del usuario y de su servidor se encuentra cifrada y protegida.

Transport Layer Security (TLS). Es considerada como la siguiente generación del Certificado TLS; permite y garantiza el intercambio de datos en un entorno seguro y privado entre dos entes, el usuario y el servidor, mediante aplicaciones como HTTP, POP3, IMAP, SSH, SMTP o NNTP. Es un sistema que está basado en el último certificado TLS y funciona de manera muy similar, básicamente: encripta la información compartida. En el protocolo TLS, se lleva a cabo un canal seguro y cifrado entre cliente y servidor en donde se negocia la criptografía del mensaje, se autentifican las claves del cifrado y se realiza una transmisión segura.

En el protocolo TLS se utiliza tanto criptografía asimétrica como simétrica. La primera se utiliza para realizar el intercambio de las claves, que a su vez serán usadas para cifrar la comunicación mediante un algoritmo simétrico. En el caso de los sitios web, para el funcionamiento de este protocolo, lo que se necesita utilizar es un certificado TLS. El servidor web tendrá instalado uno y cuando un cliente intente acceder a él, le remitirá el mismo con la clave pública del servidor, para enviar de esta forma la clave que se usará para realizar la conexión de manera segura mediante un cifrado simétrico.

El protocolo TLS /TLS no sólo proporciona confidencialidad en la información, también garantiza su integridad. Para ello se vale de un código de autenticación de mensaje (MAC, Message Authentication Code). Este código se calcula mediante una función hash con una clave secreta que sólo conocen el emisor y el receptor de la comunicación (el cliente y el servidor). De esta forma, si un sólo bit de toda la información es modificado, el MAC será totalmente diferente, y ambas partes podrían saber en ese punto que la información ha sido modificada.

Copias de seguridad. Los operadores de pasarelas de pago también pueden hacer uso del backup, que consiste en una copia de los datos originales que se realiza con el fin de disponer de un sistema

de respaldo en caso de pérdida, deterioro o robo de información. Un sistema de copias de seguridad puede hacer que una pasarela de pago que se ha visto afectada por un fallo de seguridad pueda recuperar su actividad diaria.

CVV2: Es una medida de seguridad que se requiere para las transacciones y que se encuentra en la parte frontal de la tarjeta de crédito. Está conformado por cuatro (4) dígitos visibles en la parte posterior de la tarjeta junto a la banda magnética. Si sólo se implementa esta medida de seguridad no se conseguirá la seguridad necesaria, ya que el CVV está impreso en la tarjeta y cualquier persona que tenga acceso a ella tendrá acceso a la única medida de seguridad.

3DSecure: Este sistema de seguridad está promovido por Visa y MasterCard. Al implementar el sistema 3DSecure en la pasarela de pago, los negocios ya no son los responsables de las devoluciones a causa de las reclamaciones de fraude por parte de los propietarios de la tarjeta.

Este sistema de verificación transfiere la responsabilidad de una reclamación por fraude a la entidad que emitió la tarjeta. Es necesario confirmar los términos exactos en el desplazamiento de la responsabilidad con la entidad bancaria de la tienda virtual.

El sistema 3DSecure verifica que el cliente que está realizando la compra es el verdadero titular de la tarjeta. Antes de terminar el proceso de compra el cliente debe de introducir un número PIN que solo él debe saber por lo que no podrá terminar el proceso de compra alguien que no sea su propietario. El número PIN pedido por el sistema 3DSecure puede ser de tres tipos dependiendo del protocolo de seguridad que tenga asignado la entidad bancaria propietaria de la tarjeta:

- 1. Número PIN de la tarjeta: el mismo número que solicitan los cajeros cuando se hace cualquier operación;*
- 2. Número PIN específico: número PIN especial y que es necesario solicitar al banco emisor de la tarjeta. El uso de este número PIN es común en la banca online;*
- 3. Número PIN enviado por SMS: número PIN enviado por mensaje de texto o SMS al teléfono del propietario de la tarjeta. Este número PIN es válido para un único uso.” (Rincón, 2018)*

Idoneidad

Sobre la idoneidad, debemos tener en cuenta:

Tener certificación en la norma PCI DSS y cumplirla de acuerdo con su nivel de transacciones;

Contar con sistemas de pre-validación y validación a las transacciones recibidas de comercios;

Garantizar su responsabilidad de mantener los índices de siniestralidad controlados ante los comercios que negocian con ellas;

Reportar periódicamente los comercios que se encuentran afiliados a ellos, con fines estadísticos. Así mismo, éste los evalúa a cada uno, los procesos realizados.

Contratar pólizas de seguro de directores y administradores, Infidelidad y riesgos financieros, daños materiales y responsabilidad extracontractual, así como una póliza de riesgo cibernético.

Tener un capital que atienda al nivel de riesgo operacional, crediticio y legal, el cual no necesariamente corresponderá al total de volumen transaccional. (Rincón, 2018).

4.7. Políticas y estándares

“Se recomienda como buena práctica para las Pasarelas:

Garantizar que los operadores tengan un soporte disponible y accesible, si enfrentan algún problema. El operador tiene que identificar el tipo de soporte que se ofrecerá (correo electrónico, centro de llamadas, etc.), la capacidad de respuesta del soporte ofrecido y el costo involucrado en el mismo;

Establecer políticas claras para la vinculación de los comercios, las cuales deberán atender lo desarrollado por la CE 8 de 2018 y especialmente la firma y/o aceptación de los términos y condiciones de la Pasarela.

Definir una política de prevención de lavado de activos y financiación del terrorismo que precise los lineamientos, controles y acciones necesarios para protegerse del riesgo de LA/FT, atendiendo al ambiente no presencial en el que operan las pasarelas de pago; para esto, las pasarelas deberán establecer procesos de conocimiento al cliente expeditos y con un mínimo de documentación que permita el cotejo de identidad y de origen de sus recursos, preferiblemente a través de mecanismos electrónicos tales como consultas en fuentes públicas o bureaus de crédito.

Desarrollar procesos para identificar, medir, controlar y monitorear el riesgo de LA/FT;

Evaluar el cumplimiento técnico y la efectividad de los estándares internacionales en materia de gestión de riesgos de LA/FT1;

Cumplir con los estándares de debida diligencia, implementando mecanismos para lograr una debida diligencia en el conocimiento del cliente, sin recurrir a los mecanismos tradicionales (entrevista, formulario);

Definir una política de sanciones por el incumplimiento o violación a las políticas de prevención de LA/FT;

Desarrollar una metodología para la detección de operaciones inusuales, intentadas y sospechosas, y el oportuno y eficiente reporte de estas últimas a las autoridades competentes;

Los operadores de pasarelas de pago deben aplicar estándares mínimos para la adecuada atención y manejo del fraude.

Generar un canal de comunicación para facilitar el canje de información relevante entre la pasarela y las entidades, en desarrollo de la actividad de intercambio de información;

Notificar al operador, cuando se bloquea una transacción en un sistema antifraude por considerarla de alto riesgo o sospechosa, las razones por las que se niega la transacción.

Estructurar el modelo gerencial, estratégico y operativo del Procesador de Información de Fraude de tal manera que se asegure su puesta en marcha y su seguimiento a través de indicadores de gestión y un esquema de mejoramiento de oportunidades;

Registrar la operación de anulación en el sistema de información de las redes para que posteriormente las entidades sean notificadas y apliquen los cambios respectivos en el estado de cuenta del cliente;

Diseñar dentro de la relación contractual con el comerciante, un mecanismo de confirmación de información para indagar detalles de la transacción en disputa antes de gestionar un contracargo;

Definir dentro de la relación contractual con el comerciante, un tiempo límite en el análisis de los contracargos, reversiones y anulaciones para que el cliente tenga una respuesta clara sobre su reclamación;

Establecer dentro de la relación contractual con el comerciante, un protocolo de comunicación en el proceso de contracargos para que se dé un flujo de comunicación adecuado y expedito de tal manera que el cliente tenga claridad sobre a quién dirigirse y la evolución de su caso entre otros aspectos.” (Rincón, 2018).

4.8. Diagrama de casos de uso

Para el diseño de un software se debe modelar diagramas de casos de uso para realizar una descripción de la pasarela de pagos desde el punto de vista del usuario, con esto delimitamos todos los requerimientos del aplicativo.

Diagrama de Casos de Uso General

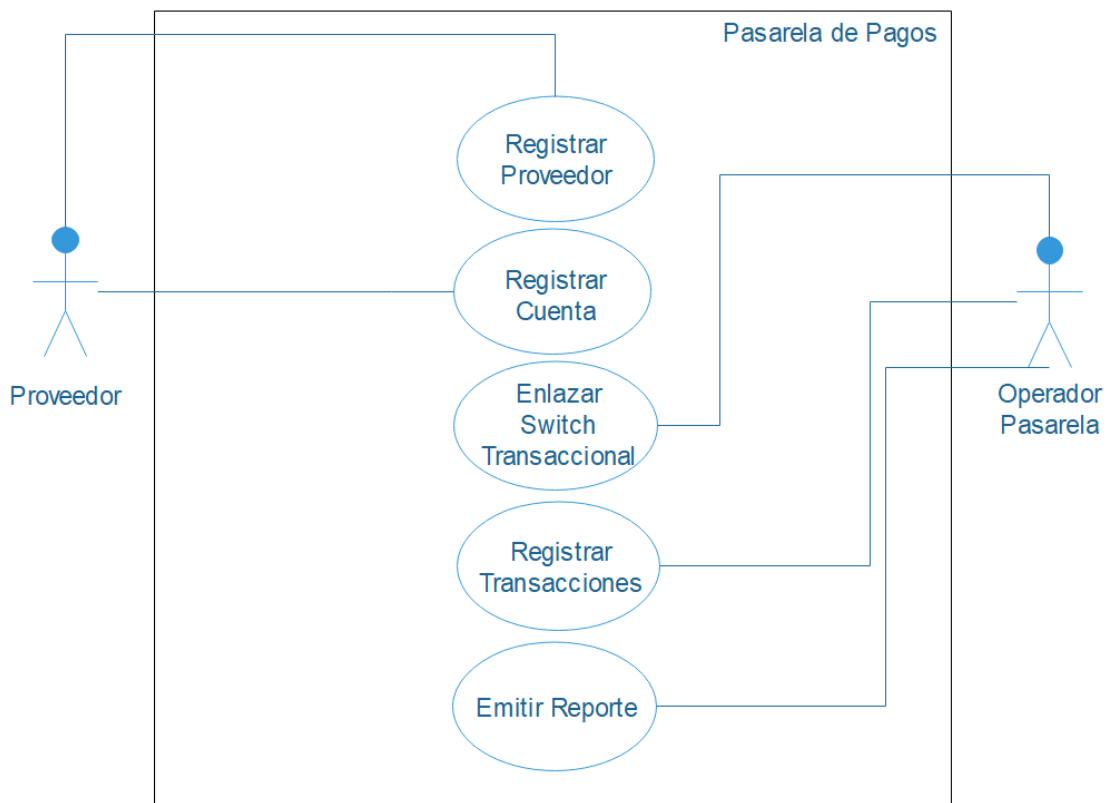


Figura 4 – 01 Diagrama de casos de uso generalizado (García, 2020)

El diagrama de casos de uso a detalle por cada uno de los actores con cada acción se lo presenta como anexo.

4.9. Diagrama de clases

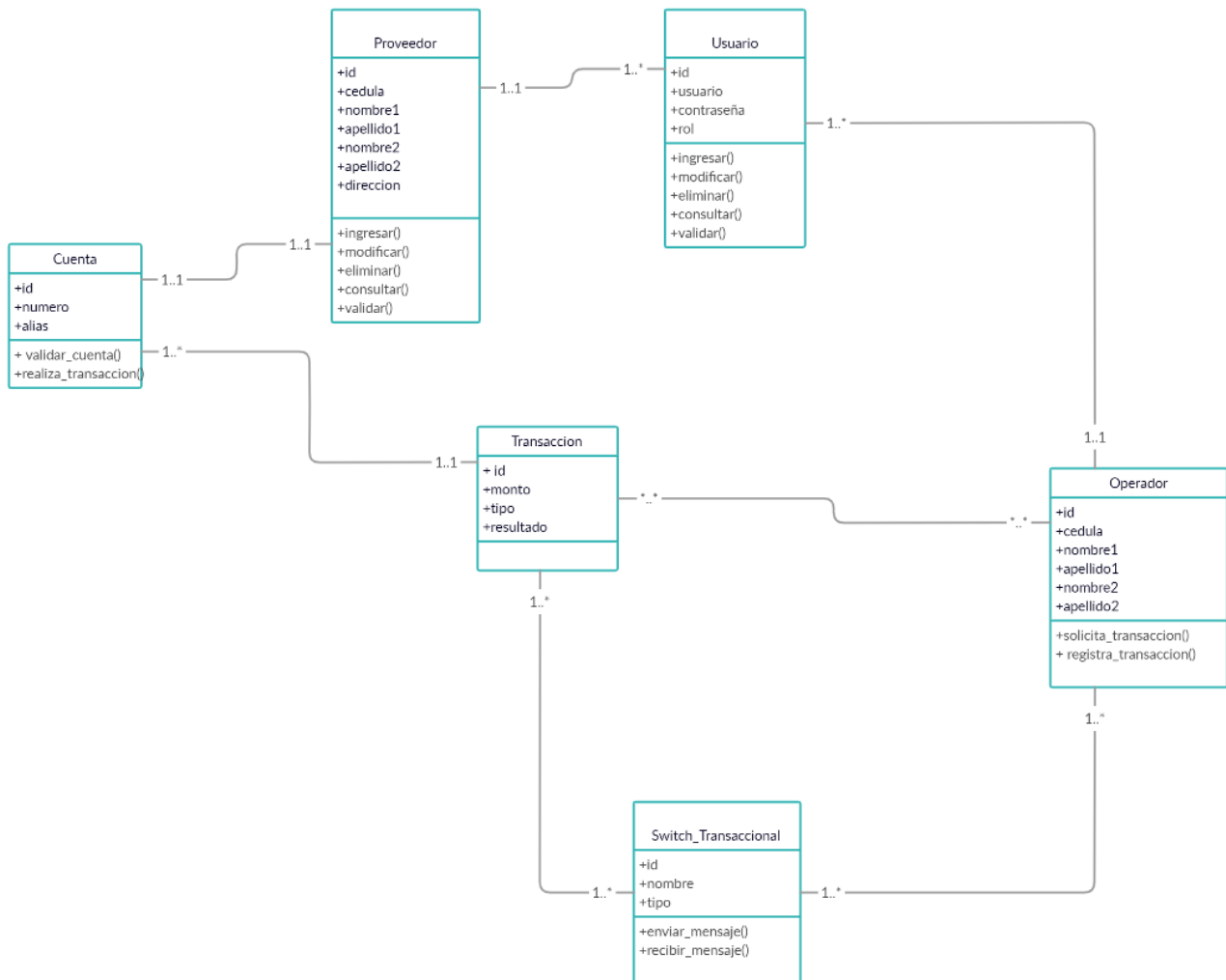


Figura 4 – 02 Diagrama de clases pasarela de pagos (Garcia, 2020)

Para poder comprender el alcance a nivel técnico de la propuesta utilizamos un diagrama de clases, tomando en cuenta todos los atributos que van a existir en cada una de ellas, con esto se comprende el sentido que tienen al relacionarse entre sí.

5. Conclusiones y Recomendaciones

5.1. Conclusiones

El Ecuador no cuenta con un manual de buenas prácticas de pasarelas de pago.

No existe una pasarela de pago desarrollada totalmente en el país.

Las pasarelas de pagos existentes en el Ecuador son franquicias de corporaciones regionales y mundiales para procesamiento de pagos en línea.

Un Switch Transaccional permite tener menores comisiones por servicio transaccional que trabajarlo directamente con las entidades financieras.

Con la implementación de una pasarela de pago propia en un negocio se puede evitar gastos de servicios mensuales permitiendo tener un costo - beneficio en el futuro.

Para la mejor interacción entre proveedor y pasarela, además, del manejo de grandes cantidades de información se necesita un operador de pasarelas de pagos.

Todas las transacciones y emisiones de reportes de las mismas se deben hacer dentro del marco regulatorio de la ley del Ecuador, aplicando tanto para el proveedor como para el operador de la pasarela de pagos.

Los estándares de seguridad de una pasarela de pagos deben existir desde el manejo de la información, infraestructura física y talento humano.

Para el manejo de riesgos de una pasarela de pagos se debe hacer una valoración y realizar un plan de contingencia para mitigar los mismos.

Las políticas y estándares de una pasarela de pagos se deben basar en casos de éxito internacionales y adaptarlos a nuestra realidad.

El software de apoyo tanto para codificación como modelado permite tener un sin número de características funcionales cuando se usa herramientas con licencia estudiantil.

El caso de estudio permite analizar tanto desde el ámbito técnico de la carrera de Ingeniería en Sistemas y Computación hasta el de Economía y Jurisprudencia por su marco económico y legal.

5.2. Recomendaciones

Se recomienda a la Super Intendencia de Bancos como ente regulador financiero del Ecuador realizar un manual de buenas prácticas de pasarelas de pago.

Se recomienda a partir de este estudio de factibilidad técnico implementar una pasarela de pago en nuestro país que reduzca las comisiones por transacciones en línea de productos o servicios.

Se recomienda que se profundice la investigación sobre los switch transaccionales dentro del Ecuador.

Se recomienda que a partir de esta propuesta técnica se analice la posibilidad de implementación de pasarelas de pagos propias para las empresas proveedoras de servicios.

Se recomienda analizar la posibilidad de contratar a operadores de pasarelas de pagos para el manejo de grandes cantidades de datos.

Para la implementación de una pasarela de pagos se recomienda acogerse a las leyes vigentes dentro del Ecuador.

Se recomienda para mitigar los riesgos en una pasarela de pagos tener planes de contingencia y un capital de riesgos para toma de acciones.

Se recomienda que a partir de casos de éxito adaptar a la realidad del Ecuador las políticas y estándares de pasarelas de pagos.

Se recomienda a la Escuela de Sistemas de la Pontificia Universidad Católica del Ecuador apoyar a los estudiantes que realicen proyectos de plataformas en línea debido a la coyuntura existente por la emergencia sanitaria.

Se recomienda a los estudiantes de la carrera el uso de herramientas de codificación, modelado de software con licencia estudiantil o software libre.

Se recomienda fomentar en las carreras de tecnologías de información el aprendizaje basado en casos reales, casos nacionales y casos globales.

Se recomienda a las carreras de Economía y Jurisprudencia ampliar los casos de estudio para el comercio electrónico y pasarelas de pagos por la importancia que va creciendo con el avance tecnológico y las nuevas necesidades que se crean por parte de los consumidores.

6. Bibliografía

- Apple. (26 de Octubre de 2019). *Descripción general de la seguridad y la privacidad de Apple Pay*. Obtenido de Apple: <https://support.apple.com/es-es/HT203027>
- Béjar, D., Luzuriaga, E., & Echeverría, F. (2006). *SWITCH TRANSACCIONAL BASADO EN EL PASO DE MENSAJES XML*. Obtenido de <https://www.dspace.espol.edu.ec/bitstream/123456789/761/1/1410.pdf>
- Cevallos, K. (2015). *UML: Casos de Uso*. Obtenido de INGENIERÍA DEL SOFTWARE: <https://ingsoftwarekarlacevallos.wordpress.com/2015/06/04/uml-casos-de-uso/>
- Cnet. (12 de 02 de 2020). *Edraw Max*. Obtenido de Cnet: https://download.cnet.com/Edraw-Max/3000-2191_4-10641613.html
- Digital Guide Ionos. (23 de 08 de 2019). *6 herramientas UML para cualquier ocasión*. Obtenido de Digital Guide Ionos: <https://www.ionos.es/digitalguide/paginas-web/desarrollo-web/las-mejores-herramientas-uml/>
- e-commerce-que-es*. (2015). Obtenido de way2ecommerce: <https://way2ecommerce.com/e-commerce-que-es>
- Educalingo. (Abril de 2020). *E-wallet*. Obtenido de Educalingo: <https://educalingo.com/es/dic-en/e-wallet>
- García, J. (2020). *Factibilidad Técnica para Desarrollo de una Pasarela de Pagos...* Quito: PUCE.
- Google presenta Android Pay, un reemplazo para su aplicación de billetera en dispositivos móviles*. (28 de Mayo de 2015). Obtenido de The Verge: <https://www.theverge.com/2015/5/28/8661867/google-introduces-android-pay-replace-wallet-app>
- Gutierrez, J. (Septiembre de 2006). *Que es un Framework*. Obtenido de lsi: http://www.lsi.us.es/~javierj/investigacion_ficheros/Framework.pdf
- Hernandez, R. (2019). *PASARELAS DE PAGO PARA ECUADOR EN 2020*. Obtenido de ronaldcreate: <http://ronaldcreate.com/3-pasarelas-de-pago-para-ecuador-en-2019>
- Huidrobo, J. M. (2017). *Telecomunicaciones. Tecnologías, Redes y Servicios. 2ª edición actualizada*. Ra-Ma.
- Paypal, una historia de éxito*. (Abril de 2017). Obtenido de soltekonline: <http://news.soltekonline.com/a/paypal>
- Perez, A. (12 de Febrero de 2019). *Medios de pago: historia y evolución de todos los métodos*. Obtenido de Directivosyempresas.com:

<https://www.directivosyempresas.com/empresas/reportajes/medios-de-pago-historia-y-evolucion/>

Quelle, L. (Febrero de 2020). *Los métodos y pasarelas de pago más populares en el ecommerce*. Obtenido de ecommerce-news: <https://ecommerce-news.es/los-metodos-y-pasarelas-de-pago-mas-populares-en-el-ecommerce-114159>

Rincón, E. (2018). *Manual de Buenas Prácticas de las Pasarelas de Pago en Colombia*. Obtenido de Observatorio eCommerce: <https://www.observatorioecommerce.com.co/wp-content/uploads/2018/10/Manual-Buenas-Practicas-Pasarelas.pdf>

Solis, D., Roque, W., & Morilla, M. L. (2013). *PASARELA DE PAGOS PARA LA SEGURIDAD DE TRANSACCIONES BANCARIAS EN LINEA*. Obtenido de 3ciencias: <https://www.3ciencias.com/wp-content/uploads/2013/08/pasarela-de-pagos.pdf>

Super Intendencia de Bancos. (8 de Abril de 2020). Obtenido de Super Intendencia de Bancos: <https://www.superbancos.gob.ec/bancos/glosario-de-terminos/>

TPVVIRTUAL. (Junio de 2019). *¿Qué es una pasarela de pagos? ¿Cómo funciona?* Obtenido de TPVVIRTUAL: <https://www.tpvvirtual.net/es/blog/pagos-digitales/que-es-pasarela-pagos-como-funciona>

Xataka. (17 de Abril de 2017). *Amazon Pay llega a España: esto es todo lo que tienes que saber sobre él*. Obtenido de Xataka: <https://www.xataka.com/servicios/amazon-pay-llega-a-espana-esto-es-todo-lo-que-tienes-que-saber-sobre-el-sistema-de-pago-online>

Xataka. (19 de Junio de 2019). *Google Pay: qué es, cómo configurarlo y bancos compatibles*. Obtenido de Xataka: <https://www.xataka.com/basics/google-pay-que-como-configurarlo-bancos-compatibles-similar>