Revista de investigación
Editada por Área de Innovación y Desarrollo, S.L.

Envío: 24/06/2013

Aceptación: 1/07/2013

Publicación: 29/08/2013

PASARELA DE PAGOS PARA LA SEGURIDAD DE TRANSACCIONES BANCARIAS EN LINEA

PAYMENTS GATEWAY FOR THE SECURITY OF ONLINE BANKIN TRANSACTIONS

Damaris Solis Fonseca[1]

Wilfredo Roque Pérez[2]

María Lourdes Morilla Faurés[3]

1. Profesor/ Especialista en Facultad Regional Granma de la Universidad de Ciencias Informáticas. Departamento Soluciones de Gestión.

2. Ingeniero en Ciencias Informáticas.

3. Profesor en la Universidad de Ciencias Informáticas. Centro de Desarrollo Cised.

RESUMEN

Las pasarelas de pagos son sistemas de pago electrónico que permiten la realización de pagos y transferencias entre tiendas electrónicas y entidades bancarias de manera segura. Se encargan de cifrar la información confidencial que se requiere para ejecutar transacciones bancarias por las redes. El artículo describe la creación de uno de estos sistemas para ser usados por bancos cubanos y tiendas electrónicas del país. Para su desarrollo se utilizaron tecnologías modernas guiándose por una metodología ágil de desarrollo de software. La pasarela creada cuenta con requisitos de seguridad que impiden el acceso no deseado por atacantes al sistema. Con el uso de la pasarela de pagos, en Cuba se apoyará a los sistemas tradicionales de cobro, facilitándose a los usuarios de internet una mayor rapidez y accesibilidad a los mismos y de forma segura.

ABSTRACT

The payment gateways are electronic payment systems that permit the making of payments and transfers between banks and electronic shops safely. They cater to encrypt sensitive information that is required to perform banking transactions over networks. The article describes the creation of one of these systems for use by Cuban banks and electronic shops in the country. To develop modern technologies were used guided by an agile methodology of software development. The gateway has established security requirements that prevent unwanted access by attackers to the system. Using the payment gateway in Cuba will support traditional billing systems, making it easier for Internet users greater speed and accessibility to them and safely.

PALABRAS CLAVE

Comercio electrónico, pasarela de pagos, seguridad, pagos, transferencias.

KEY WORDS

E-commerce, payment gateway, security, payments, transfers.

INTRODUCCIÓN

El desarrollo de la informática ha dado paso al surgimiento de las Tecnologías de la Información y las Comunicaciones (TICs), el constante uso de estas tecnologías han hecho imprescindible las prácticas diarias del Comercio Electrónico. El mismo consiste en la compra y venta de bienes y servicios utilizando medios electrónicos.

Millones de personas a través de sus computadoras hacen uso de los sitios de comercio electrónico para realizar compras de bienes o productos, pagar servicios del hogar, reservar viajes a lugares turísticos, venta o alquiler de casas, cobrar seguro de vida o de carro, entre otros servicios que les sean de interés.

Con el uso del comercio electrónico se realizan transacciones bancarias *online*[1]. Estas son operaciones bancarias que personas y empresas manejan desde sitios de comercio electrónico. Una vez que el cliente (persona que practica comercio electrónico) es usuario de un sitio web comercial (o tienda virtual como también se le llama), usando tarjetas de crédito o débito puede efectuar pagos de servicios solicitados o transferencias hacia otras cuentas bancarias. Estos procesos involucran a los bancos que gestionan las cuentas de los usuarios y de los vendedores (empresa que oferta los productos en las tiendas virtuales), y están asociadas a sus tarjetas de crédito o débito.

Los procesos de pago y transferencia bancaria *online* implican una alta seguridad en la transmisión de la información electrónica que se intercambia entre las entidades comerciales y los bancos. Tal es así que se han identificado diferentes brechas como *robo de información, suplantación de identidad* y hasta *modificación de la información*, lo que ha provocado la desconfianza en los usuarios al utilizar los sitios web comerciales como vía para gestionar sus cuentas bancarias.

Para solucionar los problemas de seguridad existen pasarelas de pagos que constituyen sistemas de pago electrónico que garantizan autenticidad, confidencialidad, integridad y el no repudio[2] en la red.

Actualmente en Cuba existe muy poco desarrollo del comercio electrónico. Como país subdesarrollado, no existen los recursos financieros para explotar su avance. A esto se le suman la brecha digital que existe a escala mundial, y la implantación del bloqueo económico[3]. Este constituye un obstáculo ya que no permiten las transacciones entre Cuba y otros bancos en el mundo. El país cuenta con varios sitios de comercio electrónico que utilizan pasarelas extranjeras, lo que implica:

- Que las tiendas virtuales operen hacia el exterior del país o para el sector turístico en la isla, ya que son los que tienen más acceso a internet.

- Por cada transacción realizada se cobra un porciento de lo pagado o una tasa fija que provoca al vendedor pérdidas monetarias por el uso de este servicio.

- Descontento por parte del cliente debido al pago por inscripción en la pasarela por el gasto de un servicio que en ocasiones no es seguro. Al ofrecerle un servicio a un cliente se debe asegurar su plena satisfacción para cerciorarse que el mismo vuelva a solicitarlo.
- Se imposibilita realizar las operaciones con la moneda de intercambio cubana ya que estas pasarelas no se comunican con las instituciones bancarias cubanas debido al bloqueo económico por parte de los EE.UU hacia Cuba.
- En los bancos cubanos se dificulta el uso de sistemas de pago electrónico para ejecutar transacciones desde sitios comerciales. Esto implica que las personas realicen sus pagos y transferencias de la forma tradicional, asistiendo a las instituciones de forma personal, obviando las múltiples ventajas que trae consigo la banca y el comercio electrónico. Con esto se ven limitadas muchas operaciones de este tipo por afectar el tiempo e incluso la distancia a la que se encuentren los clientes del banco.

Para darle solución a los problemas antes descritos se traza como objetivo general: Desarrollar una pasarela de pagos que permita realizar los procesos de pagos y transferencias bancarias online entre bancos cubanos y aplicaciones de comercio electrónico, permitiendo el uso de la moneda de intercambio cubana de manera segura y sin implicar costos.

1. Significado en inglés de: *en línea.*
2. Evita que el usuario niegue que cierta transacción tuvo lugar.
3. Impuesto por parte del gobierno de EE.UU hacia Cuba.

1.1 TRANSACCIONES BANCARIAS ON-LINE

Para la economía y el comercio, una transacción es una operación de compra y venta, o sea, el traspaso de efectivo desde una cuenta bancaria hacia otra. El comercio electrónico siendo la compra por internet, es una de las grandes ventajas que ofrece la misma a los usuarios que la usan. Esta vía de comercio resulta decisiva a pesar de que algunas personas prefieran las compras tradicionales. Esto se incrementa todavía más en el caso de personas con dificultades para la movilidad y el desplazamiento, o simplemente para los muchos casos en los que los horarios de trabajo dificultan acceder a los establecimientos en sus horarios normales.[1]

Una transacción electrónica no es más que un contrato celebrado mediante medios electrónicos, a través de la red. La mayoría de estas son enajenaciones, definidas como cualquier acto de disposición por el que se transmita la propiedad a título oneroso, entre las que se mencionan la compra-venta y el suministro.[2]

La Banca Electrónica (*E-Banking*) surge con el desarrollo del comercio electrónico, es el reflejo del banco tradicional pero desplegado a través de internet. Su uso permite un rápido y cómodo acceso a servicios bancarios como: revisar su saldo bancario, transferir dinero entre cuentas y pagar sus cuentas. Este intercambio de información financiera hacia los bancos electrónicos constituye lo que son las transacciones bancarias online. El banco virtual tiene ventajas sobre el tradicional pues permite: un amplio marco geográfico, rapidez y simplicidad en las transacciones, mayor control sobre las cuentas, mejor servicio al cliente, no requerimiento de presencia física y los servicios están disponibles todo el tiempo que se requiera sin importar hora o lugar donde se encuentre el cliente.[3]

1.2. SEGURIDAD EN LAS TRANSACCIONES BANCARIAS ONLINE

Cuando se realizan transacciones bancarias *online* se debe tener un estricto control de los mecanismos de seguridad que protegen el sistema de ataques a la autenticidad, confidencialidad, integridad, disponibilidad y el no repudio de la información (son los llamados pilares de la seguridad informática). [4]

La comunicación establecida entre las entidades y/o usuarios participantes en estas acciones debe realizarse sobre estrategias bien conocidas por ambas partes.

Utilizar conexiones a través de un servidor seguro haciendo uso de protocolos seguros permite que la información viaje cifrada entre el ordenador cliente y el servidor. Esta estrategia evita que los datos sean interceptados por terceras personas, comprometiendo datos sensibles. Al establecer una infraestructura de clave pública con sus procedimientos y mecanismos se fomenta la seguridad entre las entidades participantes cuando se realizan transacciones bancarias *online*.

1.3. PROTOCOLOS DE SEGURIDAD

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).

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.

1.4. CRIPTOGRAFÍA

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).[5]

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.[6]

1.5. REQUISITOS DE COMUNICACIÓN ENTRE LAS ENTIDADES

Para poder integrar una pasarela de pagos se debe poseer una tienda virtual que tenga como mínimo los siguientes requisitos: registro y autenticación de clientes, proceso de compra, determinación del costo, módulo integrador con la pasarela de pagos. Además la tienda virtual debe poseer políticas de venta, envíos, devoluciones y privacidad aprobadas por la pasarela de pago que se seleccione. Cada pasarela de pagos cumple con una serie de requisitos técnicos, que se verifican antes de auditar la tienda virtual. [7]

La comunicación entre una pasarela de pagos y el banco emisor de las tarjetas se puede realizar por medio de la norma ISO 8583 que proporciona un conjunto de reglas para la definición de protocolos en el intercambio de mensajes de transacciones financieras. Es un sistema de mensajes que adopta un formato uniforme para la integración, la interoperabilidad y el intercambio seguro de claves y otros propósitos administrativos.

2. PASARELAS DE PAGOS

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.

El proceso de pago utilizando las pasarelas consta de varias fases. El cliente accede a un sitio de comercio electrónico y elige la lista de artículos a comprar. La aplicación calcula el importe a cobrar y cuando el cliente está listo para pagar, es dirigido a la pasarela, la cual le muestra el monto a pagar y los datos a introducir como el número de tarjeta. La pasarela se encarga de codificar la información la cual viaja de forma segura hacia el banco. En este se comprueba rápidamente que la tarjeta sea válida (que no sea robada o que esté caducada) y que el cliente tenga los fondos suficientes para comprar los artículos. De estar todo en orden se ingresa el dinero en la cuenta del vendedor, la misma debe pertenecer al banco en cuestión o este debe tener relación con el banco que posee la cuenta del vendedor. La pasarela le comunica al comercio y al cliente el resultado de la transacción (si el pago se efectuó o no).

El proceso de transferencia sería similar: el cliente se encargará de informar a que cuenta desea ingresar la transferencia, la pasarela manipulará la información para que viaje confidencial hacia la cuenta destino, si no se presentan inconvenientes o si se presentaran, el cliente siempre será notificado. Finalmente todas las transacciones realizadas se actualizan en la base de datos de la pasarela.

2.1. PASARELAS DE PAGOS INTERNACIONALES MÁS UTILIZADAS

Actualmente existe gran diversidad en todo el planeta en cuanto a pasarelas de pagos se refiere. Cada una de ellas se diferencia entre sí por los requisitos que cumplen, el costo que cobran por transacciones, y los países con los cuales trabajan.

Paypal es una pasarela de pagos de intermediación financiera que permite realizar compras y ventas *online* de forma segura. Es la más conocida a nivel mundial y pertenece a los Estados Unidos (EE.UU). Compone el procesador de pagos en línea ideal para practicar comercio electrónico y está extendida a más de 50 países. Su servicio permite la transferencia de dinero entre usuarios que tengan correo electrónico; es una alternativa a los tradicionales cheques o giros postales. Con el uso de esta pasarela se pueden realizar peticiones de pago en comercio electrónico de sitios web de terceros, lo cual implica un sistema de validación de pagos *online* portable y adaptable. Los métodos de transferencia y pago por medio del correo electrónico tienen asociado una tarjeta de crédito (tales como Visa, Mastercard, American Express y Diners de compradores de EE.UU y Europa). Estos procesos son rápidos y seguros, debido al protocolo de seguridad SSL.

2Checkout (2CO) es la segunda pasarela a nivel mundial, por su uso, calidad, seguridad y prestigio. Esta pasarela trabaja con el 95% de los países del mundo. El pago se realiza al momento de registrarse como usuario. Con esta pasarela se puede vender a todo el mundo y recibir dinero en cualquier banco. Le permite aceptar tarjetas de crédito como: Visa, Mastercard, American Express y Diners. El sistema realiza en tiempo real la verificación de la tarjeta de crédito. La información del comprador viaja encriptada con un nivel de seguridad de 128 bits (protocolo SSL), y se utilizan certificados digitales que garantizan la autenticidad de las partes implicadas y con ello la seguridad de la transacción.

E-Pagado es una empresa que ha salido en español que gestiona los pagos con el correo electrónico y con el teléfono móvil del destinatario. Permite enviar y recibir dinero de forma segura inmediata y gratuita desde cualquier cuenta bancaria o tarjetas de crédito. La pasarela trabaja con dos tipos de cuentas, una personal y otra comercial, está dirigida a pymes (pequeñas y medianas empresas) y empresas. Su sistema además de solicitar la cuenta de correo de los clientes, exige una contraseña de seguridad para acceder al servicio. Se pueden realizar compras desde los sitios web electrónicos asociados sin necesidad de enviar el número de cuenta o la tarjeta de crédito, esto supone un incremento en la seguridad y privacidad del sistema.

2.2. PROYECTO CUBANO DE PASARELA DE PAGOS

Desde el año 2007 se empezó a trabajar en Cuba en un proyecto para el desarrollo del Comercio Electrónico con tarjetas mayoristas llamado CE-Link. Fue introducido por el Banco Central de Cuba (BCC) para el pago en tiempo real de las transacciones de comercio electrónico entre los bancos comerciales, clientes y las tiendas virtuales que realizarán este tipo de comercio en el país. Posee un módulo de administración y otro de consultas con autentificación de usuario. En el módulo de consultas los bancos y tiendas virtuales pueden consultar las transacciones que han sido enviadas hacia cada una de estas entidades.

El CE-Link almacena toda la información relacionada con cada transacción de pago, y se conforman ficheros de compensación diariamente. La pasarela se probó y funciona correctamente pero aún no se ha hecho extensivo su uso a todo el país pues se necesitan los requisitos de seguridad desarrollados por el Ministerio del Interior (MININT) para garantizar autenticidad e integridad de la información entre Tienda – CE-Link y Cliente – CE-Link.[8]

3. METODOLOGÍA DE DESARROLLO

Las metodologías de desarrollo son un conjunto de procedimientos, técnicas, herramientas y un soporte documental que ayuda a los desarrolladores a construir software. Actualmente han cobrado popularidad las metodologías ágiles por sus ventajas sobre las metodologías pesadas.[9] Las metodologías ágiles están especialmente indicadas en proyectos con requisitos cambiantes y se aplican en equipos pequeños que resuelven problemas concretos.

3.1. MICROSOFT SOLUTIONS FRAMEWORK (MSF)

MSF es una metodología ágil que se compone de principios, modelos y disciplinas. Se conoce como la metodología de soluciones de Microsoft. Sirve como guía para administrar el equipo y los procesos en el desarrollo de software. Los equipos son pequeños y multidisciplinarios. Los miembros comparten responsabilidades y complementan sus habilidades para enfocarse al proyecto. Cada uno tiene un rol definido que adquiere relevancia en las distintas etapas del proceso de desarrollo. Contempla un diseño lógico en tres capas para el diseño de aplicaciones distribuidas multicapas. Define una aplicación como una red lógica de servicios distribuibles y reutilizables que cooperan en tareas comunes. Provee una estructura para el desarrollo de aplicaciones que consiste en 6 etapas distintas principales, también se pueden acortar las etapas en 4, la decisión de extender o no las etapas, depende del equipo de desarrollo y del cliente general. Cada una de las etapas culmina con una meta definida. Una primera etapa es la Visión en la que todo el equipo de desarrollo se reúne y definen la visión y el ámbito que el sistema va a tener. La Planeación es la segunda etapa en la que se especifican y definen las funcionalidades que compondrán al sistema. En la tercera etapa que es el Desarrollo es donde se crea y prueba la solución. En la Estabilización que es la siguiente etapa es donde se crea una solución piloto para el lanzamiento del producto. Finalmente se realizan la Instalación y el Soporte del producto en el lugar donde se vaya a usar. MSF para Metodologías de Desarrollo Ágil (MSF for ASD) es un proceso de desarrollo formado por escenarios. Incorpora las prácticas probadas por Microsoft con respecto a los requerimientos, diseño, seguridad, rendimiento y pruebas. Presenta una guía recomendable para gestores y desarrolladores de proyecto software adaptable a la metodología de cada empresa. El estudio realizado sobre metodologías ágiles permitió escoger a MSF for ASD como metodología de desarrollo para la creación del software. Sus modelos, principios y actividades son grandes ventajas de esta sobre las demás que se podían utilizar.[10]

4. RESULTADOS Y DISCUSIÓN

En la presente sección se muestran los resultados de la aplicación de la metodología y los elementos que se tuvieron en cuenta en cada una de las fases de desarrollo.

4.1. FASE VISIÓN Y ALCANCE

En esta fase se establece y define el dominio del problema, proporcionando al equipo de trabajo, una visión clara de los objetivos que persigue el desarrollo de la pasarela de pagos, una idea de la lógica del dominio y de las alternativas propuestas para solucionar de manera óptima el problema planteado. Es tomado como el punto de partida para el posterior diseño del sistema.

Modelo de dominio

Con la elaboración del modelo de dominio se intenta comprender los conceptos que intervienen en la pasarela de pagos. Este modelo se presenta en un diagrama UML[1] que muestra las clases del dominio, con algunos atributos y como se relacionan unas con otras mediantes asociaciones.

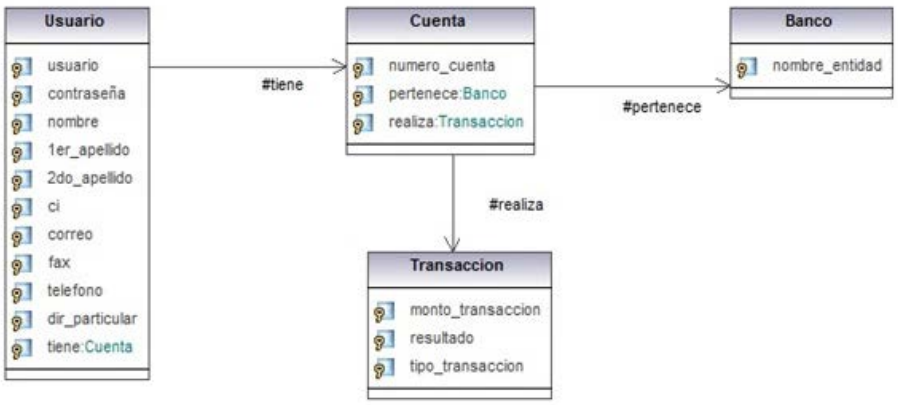

Figura 1: Modelo de Dominio. Fuente: Elaboración propia.

El modelo representa las entidades que interactúan en la pasarela de pagos para realizar transacciones bancarias en línea. Se muestra un usuario que realiza pagos o transferencias bancarias por medio de una cuenta que está asociada a la tarjeta de crédito o débito. Esta última es emitida por un banco que puede manejar las cuentas de los usuarios o se comunica con otros bancos que en ese caso controlaría estas cuentas. El usuario se registra insertando sus datos personales, creándose automáticamente una cuenta de este en la pasarela. La pasarela almacena además los datos de los bancos que emiten las tarjetas asociadas a las cuentas. Una vez que la pasarela contiene todos estos datos puede notificar a los usuarios y a los bancos de todas las acciones que se realizan por medio de esta.

4.2. FASE PLANEACIÓN

En esta fase el equipo de desarrollo prepara las especificaciones funcionales. Los principales artefactos de esta fase son los escenarios y los requerimientos de calidad del servicio que sirven de guía para todo el proceso de desarrollo.

Especificación de escenarios:

Para la correcta elaboración de la pasarela de pagos y obtener un mejor razonamiento en el momento de la implementación se especificarán y describirán los escenarios necesarios de la propuesta de solución.

Módulo Administración:

- Configurar cuenta de administración.
- Mostrar usuario de administración.
- Crear usuario de administración:
    - Notificar al administrador de la creación de la cuenta.
- Modificar usuario de administración.
- Eliminar usuario de administración.
- Cambiar contraseña de administrador.
    - Configurar cliente.
- Mostrar cliente.
- Eliminar cliente (desactivarlo).
- Buscar cliente.
- Configurar pago.
- Mostrar operaciones de pago:
    - Filtrar por fecha.
- Gestionar banco.
- Mostrar banco.
- Crear banco.
- Modificar banco.
- Eliminar banco (desactivar).

- Autenticar administrador.

  - Módulo Administración de clientes:

- Registrar cliente

  - Notificar al cliente de la creación de la cuenta.

- Configurar cuenta.
- Modificar datos del cliente.
- Eliminar cliente (desactivar).
- Cambiar contraseña.
- Autenticar cliente.
- Configurar cuenta bancaria.
- Listar cuentas bancarias.
- Registrar cuenta bancaria.
- Eliminar cuenta bancaria.
- Consultar saldo bancario.
- Mostrar reporte del historial de transacciones:

  - Filtrar por fecha.

Realizar pago.

Enviar datos del pago.

- Notificar a las entidades:
- Al vendedor.
- Al cliente.
- Registrar resultado del pago.
- Realizar transferencia.
- Enviar datos de la transferencia.
- Notificar a las entidades:
- Al vendedor.
- Al cliente. Registrar resultado de la transferencia.

Requisitos de calidad del servicio

Los requisitos de calidad del servicio son las cualidades que el producto debe tener. Adoptan la forma de restricciones sobre cómo debería funcionar la pasarela de pagos.[10]

A continuación se definen los requisitos de calidad del servicio de la pasarela de pagos:

Sobre el uso del sistema.

El sistema podrá ser utilizado por cualquier usuario con conocimientos básicos sobre el uso de una computadora.

Disponibilidad.

El sistema debe estar disponible las 24 horas los 7 días de la semana. El sistema no funcionará en caso de existir fallas o inestabilidad en las comunicaciones.

Confiabilidad.

La información manejada por el sistema está protegida de acceso no autorizado.

Integridad.

La información manejada por el sistema permanece inalterada a menos que sea modificada por el personal autorizado, esta modificación es registrada, asegurando su precisión y confiabilidad.

Confidencialidad.

Sólo se accederá a la base de datos (BD) desde la aplicación, nunca directamente desde el gestor de BD. A las funcionalidades de la pasarela acceden sólo los usuarios que posean los permisos suficientes.

Referentes a lenguajes de programación.

El sistema debe implementarse utilizando los lenguajes C#, ASP.Net, sobre la plataforma .Net usando como IDE Microsoft Visual Studio Team System 2010, Java Script y CSS para propiciarle al sitio estilo y dinamismo. Como gestor de base de datos PostgreSQL 9.1.

Interfaces de usuario.

Interfaz accesible, intuitiva y discreta. El manejo de las funcionalidades debe ser lo más intuitivo posible, de manera que sean muy claras las posibles acciones a llevar a cabo y la manera de hacerlas.

Interfaces de *hardware.*

En el cliente se requiere una máquina con 256Mb de RAM y un microprocesador de 1GHz como mínimo, puerto de conexión de red o en su defecto modem u otro dispositivo de interconexión inalámbrico. El servidor de base de datos debe contar con los siguientes requisitos mínimos: 2Gb de RAM, microprocesador 3.06 GHz en adelante y 40gb de espacio de almacenamiento en disco duro.

Interfaces de *software.*

Sistema operativo Windows XP/Vista/7, Linux, MAC; framework .NET 4.0 o superior; en el cliente se requiere tener instalado Navegador web Internet Explorer 7 ó superior, Mozilla Firefox 6.02 o superior.

Interfaces de comunicación.

Los servicios web poseerán una interfaz que permita manejar un alto nivel de seguridad haciendo uso del protocolo del nivel de aplicación HTTPS.

Requisitos de Licencia.

Para el desarrollo del sistema es necesario el uso de un conjunto de aplicaciones, que son propietarios, siendo indispensables para el buen desempeño de las mismas el tener las respectivas licencias:

- Windows 7 Ultimate edition.
- Internet Information Services 7.5
- Microsoft Visual Studio Team System 2010.

4.3. FASE DE DESARROLLO

En esta fase se describe la arquitectura para la ejecución de la pasarela de pagos definiéndose la vista lógica de la misma. Se modelan los diagramas de aplicación y lógico de centro de datos exigidos por la metodología establecida.

Vista lógica de la arquitectura

La arquitectura está representada por 3 capas lógicas, lo que permite disminuir al máximo el acoplamiento, aumentar la reutilización entre las mismas, facilitar la modularidad, reusabilidad, el cambio y la portabilidad. Esta distribución de capas permite que se realicen grandes cambios sin tener que realizar alteraciones en las demás capas. Al tener las capas una correcta definición, la comunicación entre ellas se realizará sólo a nivel de interfaces, permitiendo trabajar de manera transparente a las instancias reales.

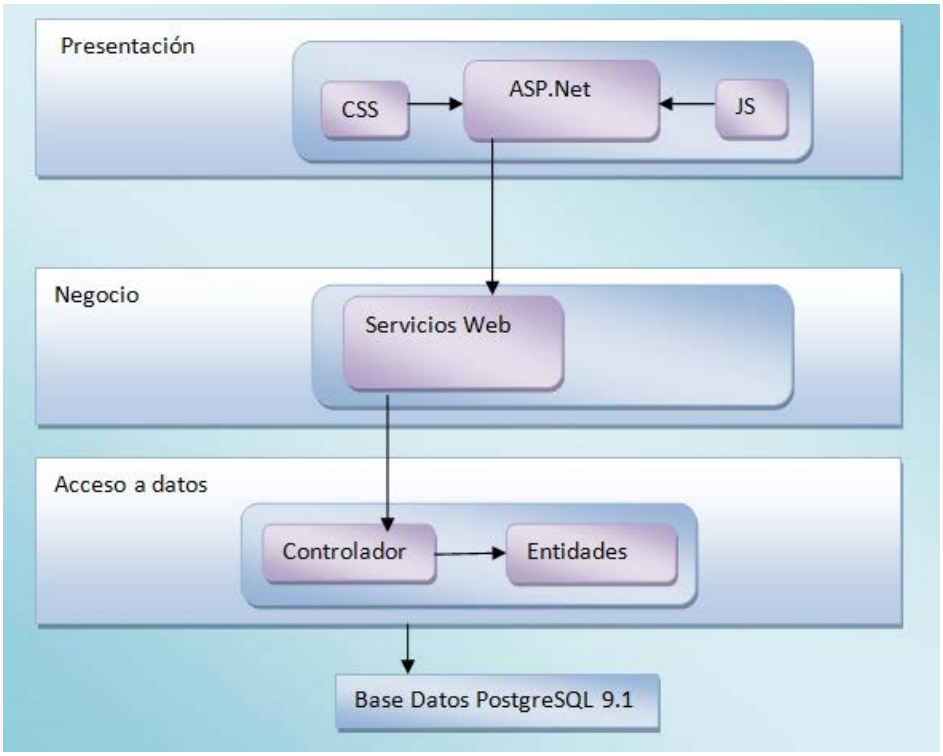

Figura 2: Diagrama de la vista lógica de la arquitectura. Fuente: Elaboración propia.

En la figura muestra la capa de presentación contiene las interfaces de usuario y los componentes para su correcto funcionamiento. Estos elementos son ficheros *JavaScript* y CSS. Además de contar con un proyecto web desarrollado con el *framework*ASP.NET MVC en su versión 2.0, teniendo comunicación directa con la capa de negocio. Con su utilización se aprovechan en esta capa las ventajas del patrón MVC.

En la capa de negocio se recogen las funcionalidades necesarias para darle solución a los requerimientos definidos estableciendo los servicios web que brinda la pasarela de pagos. Contiene las clases controladoras, que son las que manejan todas las operaciones sobre las

entidades del dominio definidas. Además se comunica con la capa de presentación, para recibir las solicitudes y presentar los resultados, y con la capa de acceso a datos, para solicitar al gestor de base de datos almacenar o recuperar datos de él. En la capa de acceso a datos se encuentran un conjunto de librerías que permiten la directa relación con las funcionalidades definidas en el dominio. Para hacer posible esta relación se utilizaron las clases interfaces y controladoras que definen a la capa de negocio, posibilitando de esta forma que se puedan hacer cambios en esta capa sin afectar a las demás capas. Su función principal es realizar la implementación de las interfaces y trabajar al mismo tiempo directamente con la fuente de datos establecida. La capa de acceso a datos se comunica con la base de datos la cual está constituida por todo el conjunto de tablas y procedimientos que permiten el almacenamiento de la información recogida y procesada.

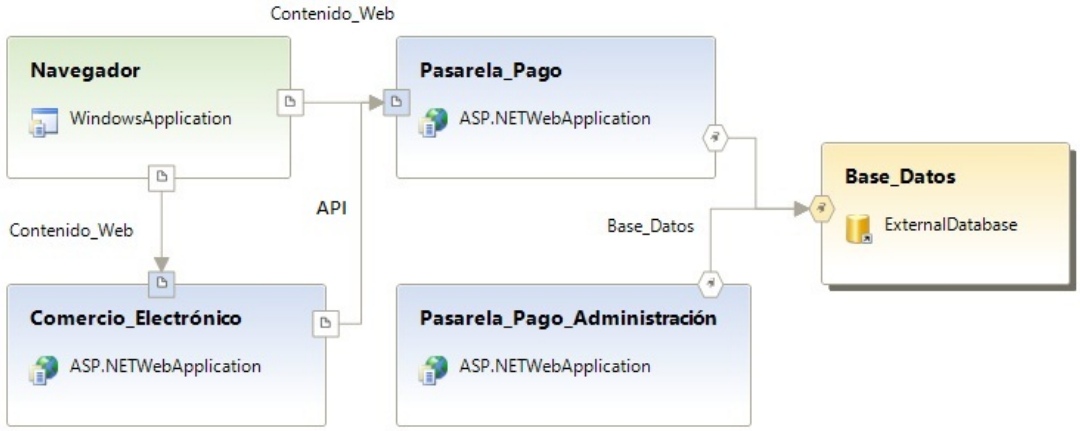

Figura 3: Diagrama de aplicación. Fuente: Elaboración propia.

El diagrama define los componentes que se relacionan con la pasarela de pagos y sus conexiones. El diagrama muestra un navegador por medio del cual los usuarios interactúan con la pasarela. Además existe otra aplicación que es la tienda virtual donde los usuarios ejecutan sus transacciones y a la vez esta tienda mantiene conexión con la pasarela a través de las API (Application Programming Interface). Son métodos que el desarrollador de cualquier aplicación ofrece a otros desarrolladores para que distintas aplicaciones puedan interactuar con su aplicación.[11] Es decir que mediante las API de la tienda virtual el cliente accede mediante un servicio web de manera segura a la pasarela de pagos. Esta a su vez se conecta a la base de datos que almacena la información manejada en ella. Por otra parte se encuentra la aplicación de Administración de la pasarela de pagos que accede a la base de datos para consultar los mismos dependiendo de las acciones a ejecutar.

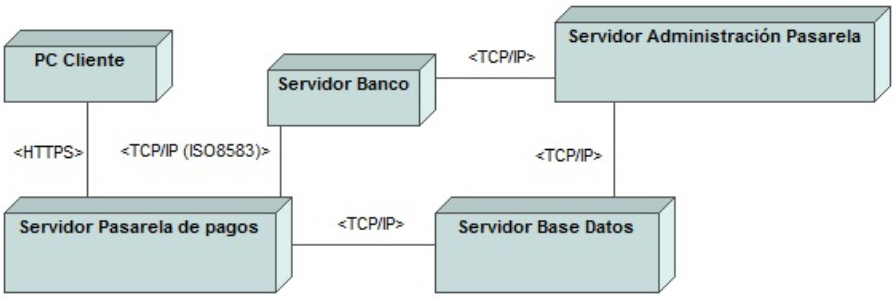

Figura 4: Diagrama lógico de centro de datos. Fuente: Elaboración propia.

El diagrama conforma las configuraciones de los servidores involucrados en la conexión con la pasarela de pagos. La figura muestra a un cliente (página web desde donde el usuario practica comercio electrónico) que se conecta por un modo seguro al servidor de aplicación de la pasarela de pagos. Al mismo tiempo el servidor de aplicación de la pasarela de pagos tiene conexión directa con el servidor de base de datos de la misma. Este último es consultado por el servidor de Administración de la pasarela de pagos. Para las conexiones entre el servidor de aplicación, el servidor de base de datos y el servidor de Administración se utilizó el protocolo seguro de transporte TCP/IP. Además el servidor de aplicaciones de la pasarela de pagos se comunica a través de un canal seguro con el banco, utilizando SSL de 128 bits, el cual garantiza la integridad de los datos que viajan. Este banco es el que maneja las cuentas de los usuarios. El protocolo de transporte utilizado es TCP/IP y los mensajes que se intercambian entre estos es por medio de la norma de intercambio de datos electrónicos ISO 8583.

4.4. FASE DE ESTABILIZACIÓN

En esta fase se definen las pruebas de calidad del software. Al software se le realizaron distintas pruebas empleando los métodos de caja blanca y caja negra. La prueba de unidad es la primera fase de las pruebas dinámicas y se realizan sobre cada módulo del software de manera independiente. Las pruebas unitarias se le aplicaron a las funcionalidades de más peso, o sea a los métodos más complejos de la pasarela de pagos.

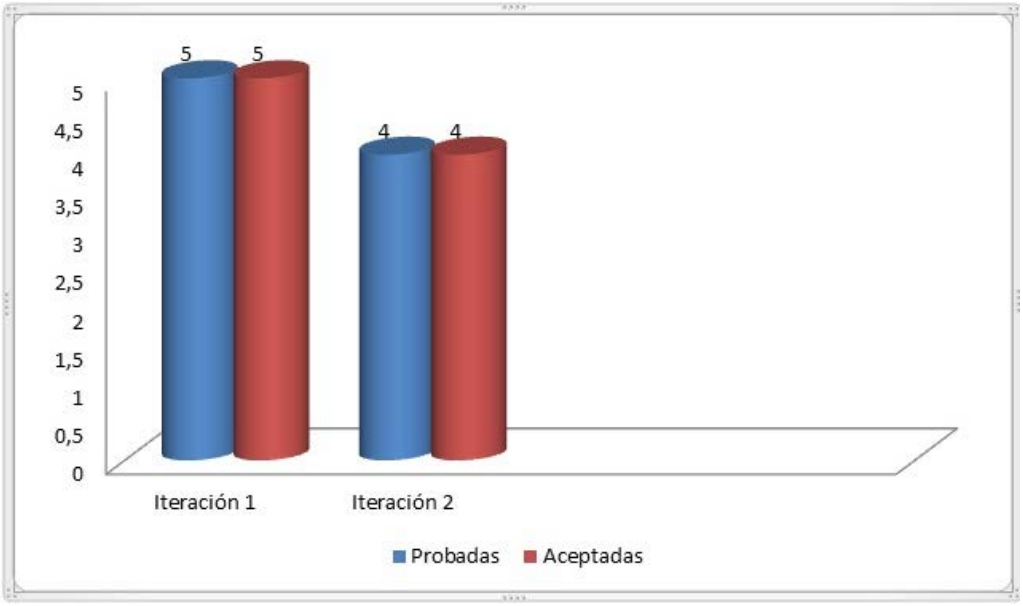

Tabla 1: Resultado de las pruebas unitarias. Fuente: Elaboración propia.

Se efectuaron dos iteraciones de pruebas unitarias a los métodos de mayor complejidad, estos pertenecen al módulo Administración de clientes. En una primera iteración se realizaron 5 pruebas de las cuales todas fueron aceptadas. En la segunda iteración se le aplicó la prueba de unidad a 4 funcionalidades de las cuelas ninguna falló.

Las pruebas de caja negra a la pasarela de pagos se efectuaron en dos iteraciones mediante la realización de casos de prueba a cada uno de los escenarios y sus tareas correspondientes. Para ello se detallaron las clases válidas e inválidas teniendo en cuenta las entradas de datos para cada una de las interfaces.

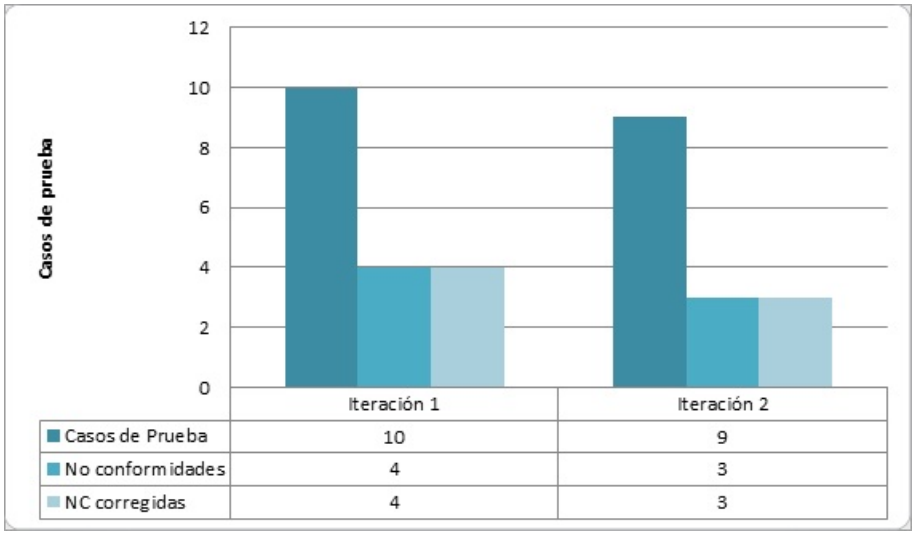

Tabla 2: Resultados de las pruebas de caja negra. Fuente: Elaboración propia.

La figura representa las pruebas de caja negras realizadas, de los 10 escenarios y las 22 tareas existentes, se identificaron 19 casos de pruebas, constituyendo estos las interfaces que requieren entrada de datos. En la primera iteración se efectuaron 10 casos de pruebas detectándose 4 no conformidades a las cuales se les dio solución. En la segunda y última iteración se detectaron 3 no conformidades de los 9 casos de prueba restantes, las mismas fueron resueltas en su totalidad. En las dos iteraciones efectuadas se detectaron un total de 13 no conformidades, las cuales en su mayoría respondían a errores de bajo impacto en el correcto funcionamiento de la aplicación y todas tuvieron solución un tiempo máximo de 2 días, lo que indica que la pasarela de pagos desarrollada presenta buena calidad.

CONCLUSIONES

El análisis bibliográfico permitió concretar el proceso de transacciones bancarias que se gestionan mediante pasarelas de pagos.

El análisis de las pasarelas de pagos estudiadas permitió definir parte de las funcionalidades en el desarrollo de la pasarela de pagos que ejecuta transferencias y pagos bancarios *online* de manera segura.

La pasarela de pagos favorece la ejecución de transferencias y pagos bancarios *online* garantizando los niveles de seguridad de la información, reduciendo a un mínimo el tiempo de respuesta.

El análisis de los mecanismos de seguridad en transacciones de comercio electrónico permitió crear una aplicación de pago para garantizar la confianza en el uso de su solución.

Se realizó el diseño de la pasarela de pagos logrando un mayor entendimiento de la misma para su posterior implementación.

Se validó la solución empleando los métodos de pruebas de caja negra y caja blanca arrojándose resultados satisfactorios como base para reconocer que la solución está en condiciones para ser liberada.

REFERENCIAS

[1] **EDUARDO BERROCAL, R.D; GIMÉNEZ, MANUEL SALA, NACHO SOMALO,** (2009) Libro Blanco del Comercio Electrónico.

[2] Texto Único Ordenado de la Ley del Impuesto a la Renta - Decreto Legislativo N° 774, artículo 5°.

[3] www.alfa-redi.org, Revista de Derecho Informático [citado 10-11-2011].

[4] **TARRATS, J.B. AND F. JORDÁN.** (2000) LA SEGURIDAD DE LAS TRANSACCIONES BANCARIAS EN INTERNET. Informes SEIS, p. 133.

[5] **BONASTRE, J.A.L.**, Seguridad en el comercio electrónico.

[6] **TELLEZ,** (2009) La Seguridad del entorno tecnológico y en las Transacciones para el Comercio Electrónico.

[7] Anónimo, 2011, APOYO DIGITAL S.A.C.

[8] Anónimo, 2007, PROYECTO PARA EL PAGO DE OPERACIONES DE COMERCIO ELECTRONICO CON TARJETAS MAYORISTAS CE-LINK.

[9] **CARRILLO PÉREZ, ISAÍAS.** (2008) METODOLOGIA DE DESARROLLO DEL SOFTWARE.

[10]Anónimo, Guía de MSF for Agile Software Development.

[11]google.dirson.com, [citado 7-5-2012].