

SISTEMA Y MÉTODO PARA TRANSACCIONES FÁCILES Y SEGURAS EN REDES SOCIALES PARA DISPOSITIVOS MÓVILES

RESUMEN:

La presente solicitud de Patente de Invención, se refiere a un sistema y un método para transacciones fáciles y seguras en redes sociales para dispositivos móviles tales como un teléfono móvil, una tableta, o cualquier otro dispositivo con acceso a internet los cuales hacen parte del sistema. Asimismo, este sistema y método para transacciones fáciles y seguras en redes sociales para dispositivos móviles mediante elementos técnicos tales como un computador u otro dispositivo electrónico con elementos de comunicación que tenga acceso a internet que se encuentran ubicados en otro lugar y que a su vez hacen parte del mismo sistema, reciben, procesan, transforman, y/o emiten datos en donde se lleva a cabo el método para realizar una transacción financiera fácil, segura e inmediata por medio de redes sociales a partir de comandos marcados con etiquetas predefinidas, que capturan información del emisor como del receptor para ser validada y posteriormente hacía el emisor generada una notificación (push) para la previa autorización de la transacción por medio de un patrón desde una aplicación Progressive Web App, en donde el sistema es la parte tangible que permite realizar el método para efectuar una transacción segura, fácil e inmediata, mediante el empleo de redes sociales.

SISTEMA Y MÉTODO PARA TRANSACCIONES FÁCILES Y SEGURAS EN REDES SOCIALES PARA DISPOSITIVOS MÓVILES

OBJETO DE LA INVENCION:

La presente solicitud de Patente de Invención, se refiere a un sistema y un método para transacciones fáciles y seguras en redes sociales para dispositivos móviles, con el fin de realizar una transacción financiera fácil, segura e inmediata en tiempo real a través de una aplicación Progressive Web App (PWA) vinculada a una red social externa a la aplicación bancaria, empleando comandos marcados con etiquetas predefinidas, que toma información necesaria tanto del emisor como del receptor de la transacción generando la validación y autorización de la transacción a través de una aplicación, que puede ser una aplicación web progresiva no nativa o una aplicación nativa convencional, esto se hace mediante la integración y la combinación de varios elementos (dispositivos móviles tales como un teléfono móvil, una tableta, o cualquier otro dispositivo con acceso a internet, un computador u otro dispositivo electrónico con elementos de comunicación que tenga acceso a internet ubicados en otro lugar) que hacen parte del sistema (hardware) que, junto con el método, permiten optimizar la validación de la identidad del usuario, manteniendo todos los protocolos de seguridad que a su vez garantizan que la transacción sea totalmente segura de acuerdo con los estándares del banco o institución financiera, en donde el sistema es la parte tangible que permite realizar el método para efectuar una transacción segura, fácil e inmediata, en un ambiente de redes sociales.

ANTECEDENTES DE LA INVENCION:

Dentro del estado de la técnica anterior, se encuentran múltiples métodos juntos con sus respectivos sistemas para realizar una transacción financiera teniendo como soporte las redes sociales, con el fin de realizar una transacción financiera sin retrasos, fácil y de manera segura, por lo cual se presentan algunos documentos de patentes que hacen parte del estado de la técnica y que al mismo tiempo hacen de punto de partida y de comparación con respecto a la invención que se desea proteger en esta solicitud, en el cual esta invención se encuentra dentro del campo tecnológico de las invenciones que se encuentran implementadas por computador que conjugan entre sí un software y un hardware para resolver el problema técnico planteado en esta solicitud.

En la patente de invención Estadounidense US 20100306099 (Diciembre 02 de 2010) del solicitante BOKU INC [US], enseña un sistema y un método para autenticar y procesar solicitudes recibidas por medio de sitios web de redes sociales, en donde el sistema definido incluye un medio de almacenamiento de datos para almacenar los datos que asocian un primer número de teléfono de un usuario con unas identificaciones del usuario en un sitio web de red social; y un intercambio acoplado con el medio de almacenamiento de datos, donde dicho intercambio incluye un procesador de formato común y una pluralidad de conversores para interactuar con una pluralidad de controladores de comunicaciones móviles. Así mismo, el método divulgado comprende los pasos de recibir en un servidor una solicitud de un usuario autenticado por un sitio web de red social; identificar un primer número de teléfono del usuario; comunicarse por el servidor con un teléfono móvil en el primer número de teléfono para confirmar la solicitud; y en respuesta a la solicitud que es confirmada por el teléfono móvil en el primer número de teléfono, procesar la solicitud usando los fondos asociados con el teléfono móvil en el primer número de teléfono.

Sin embargo, con base al método y el sistema descritos en la patente de invención Estadounidense US 20100306099 anteriormente enunciada, ilustra una desventaja, que consiste, en que requiere la comunicación del servidor con el teléfono móvil y la autenticación la hace por medio de un número de teléfono únicamente, lo cual no garantiza que la comunicación sea segura y no se establezca los protocolos de un banco o institución financiera para realizar las transacciones solicitadas.

En la patente de invención Estadounidense US 20130054458 (Febrero 28 de 2013) del solicitante MONEYGRAM INTERNATIONAL INC [US], enseña unos sistemas y unos métodos que utilizan una plataforma de red social para suministrar información de autenticación para realizar una transacción de transferencia de dinero, en donde el método puede incluir, obtener y utilizar la información de los datos del perfil de la red social en línea del remitente, receptor o ambos con el fin de facilitar una transacción conveniente y segura. Así, esta divulgación incluye una base de datos de perfil de red social en línea configurada para almacenar y correlacionar la información de perfil para múltiples usuarios y un dispositivo de procesamiento de transacción de transferencia de dinero en comunicación con la base de datos para autenticar una transacción de transferencia de dinero, en donde todas estas modalidades se implementan en internet, con aplicaciones dedicadas para un computador y/o un dispositivo móvil.

En la patente de invención Estadounidense US 9218594 (Mayo 05 de 2014) del solicitante IBM [US], enseña un método y un sistema para la realización de pagos

electrónicos asistidos en redes sociales, en donde el método incluye los pasos para determinar uno o más miembros de una red social que busca un pago hacia una contribución financiera de una transacción en tiempo real entre el usuario y un comercio; consultar uno o más miembros en un orden basado en probabilidad descendiente de contribución financiera hasta que se hayan recibido suficientes fondos para el pago de la transacción; y procesar una transferencia de dinero desde el usuario y/o cada uno de los miembros al comercio para completar la transacción en tiempo real.

En la patente de invención Estadounidense US 2018/0183737 (Junio 26 de 2018) del solicitante FACEBOOK INC [US], enseña sistemas, métodos y dispositivos para procesar transacciones de pago entre un usuario y un comercio usando un entorno de mensajería, en particular, un sistema de comercio permite que el usuario inicie una sesión de comunicaciones con un entorno de mensajería asociado con el comercio usando un lenguaje natural. Así, los mensajes enviados son analizados para identificar un producto y una solicitud de compra del producto identificado. Con base en el producto identificado y la solicitud para comprar el producto, se inicia una transacción de pago a nombre del usuario con base en una conversación de lenguaje natural y sin redirigir el usuario lejos de la sesión de comunicaciones. Adicionalmente, se puede suministrar un mensaje de inicio de pago desde el entorno de mensajería al usuario indicando que la transacción de pago ha sido iniciada.

En la patente de invención Colombiana CO 11-82169 (Junio 30 de 2011) del solicitante MTN MOBILE MONEY SA (PTY) LTD [CO], enseña un método para procesar de forma segura una transacción, en donde el método incluye almacenar una pluralidad de identificadores de instrumento de transacción financiera encriptados en una memoria en donde no hay clave de descifrado para estos almacenados en la memoria y además, en donde los identificadores de instrumento de transacción financiera están cada uno asociados con un dispositivo de comunicaciones móviles. El método también incluye recibir de un servidor una solicitud para procesar una transacción, retirar de la memoria el identificador de instrumento de transacción financiera asociado con el dispositivo de comunicaciones móviles, transmitir el identificador de instrumento de transacción financiera retirado al dispositivo de comunicaciones móviles, recibir en el dispositivo de comunicaciones móviles los datos de transacción, y usar los datos de transacción recibidos para llevar a cabo una transacción financiera.

De acuerdo a lo anterior, es claro que a pesar de la diversidad de oferta de productos y plataformas digitales móviles para la realización de transacciones en línea, actualmente es necesario que los usuarios todavía cuenten con una cuenta

bancaria en un banco o institución financiera y que la transacción se realice a través una plataforma digital emitida por dicho banco o institución financiera o servicio que media la transacción.

Lo anterior constituye claramente una limitación significativa para los usuarios y para el desarrollo de nuevos medios de comercio electrónico, toda vez que se realizan etapas adicionales en los procesos de transacción financiera por internet. En consecuencia, existe la necesidad de proporcionar un sistema y un método que permite ejecutar transacciones en aplicaciones externas a las bancarias de forma más ágil, versátil e inmediata que las que existen actualmente en el mercado, que a su vez mantienen todos los protocolos de seguridad que garantizan que la transacción sea totalmente segura de acuerdo con los estándares del banco o institución financiera.

En los documentos del estado de la técnica referenciados, enseñan parte del estado de la técnica del mismo campo tecnológico de la solicitud, tal y como se observa en las patentes de invención Estadounidenses US 20100306099, US 20130054458, US 9218594, US 2018/0183737 igualmente en la patente de invención colombiana CO 11-82169.

Con base a lo anterior, se referencian dichos documentos que hacen parte del estado de la técnica, con el fin de exponer los antecedentes de la solicitud y tomar como punto de partida las mejoras que hacen diferente la solicitud mediante sus características técnicas constructivas que solucionan el problema técnico objetivo planteado en la solicitud.

DESCRIPCIÓN GENERAL Y DETALLADA DE LA INVENCIÓN:

El problema técnico objetivo de la presente solicitud, consiste en realizar una transacción en la que se hace una transferencia de fondos de un usuario a otro directamente en una red social de manera segura, sin necesidad de elementos adicionales requeridos por un banco o entidad financiera, todo en tiempo real sin que el usuario final tenga retrasos considerables.

La presente solicitud de patente de invención tiene como objetivo aportar la solución al problema mediante un sistema y un método para transacciones fáciles y seguras en redes sociales para dispositivos móviles, con el fin de realizar una transacción financiera fácil, segura e inmediata en tiempo real a través de una aplicación de una red social externa a la aplicación bancaria, empleando comandos marcados con etiquetas predefinidas, que toma información necesaria tanto del emisor como del receptor de la transacción generando la validación y autorización de la transacción a través de una aplicación, que puede ser una aplicación web

progresiva no nativa o una aplicación nativa convencional, todo lo anterior, se hace mediante la integración y la combinación de varios elementos (dispositivos móviles tales como un teléfono móvil, una tableta, o cualquier otro dispositivo con acceso a internet, un computador u otro dispositivo electrónico con elementos de comunicación que tenga acceso a internet ubicados en otro lugar) que hacen parte del sistema (hardware) que junto con el método permiten optimizar la validación de la identidad del usuario, manteniendo todos los protocolos de seguridad que a su vez garantizan que la transacción sea totalmente segura de acuerdo con los estándares del banco o institución financiera, en donde el sistema es la parte tangible que permite realizar el método para efectuar una transacción segura, fácil e inmediata, mediante el empleo de redes sociales.

La presente invención se encuentra dentro del campo técnico de los sistemas de las comunicaciones, relacionada con las transacciones financieras en redes sociales.

La presente invención ilustra un sistema y un método para transacciones fáciles y seguras en redes sociales para dispositivos móviles tales como un teléfono móvil, una tableta, o cualquier otro dispositivo con acceso a internet el cual hacen parte del sistema. Asimismo, mediante elementos técnicos tales como un computador u otro dispositivo electrónico con elementos de comunicación que tenga acceso a internet que se encuentran ubicados en otro lugar y que a su vez hacen parte del mismo sistema, reciben, procesan, transforman, y/o emiten datos en donde se lleva a cabo el método para realizar una transacción financiera fácil, segura e inmediata por medio de redes sociales a partir de comandos marcados con etiquetas predefinidas, que toma información necesaria tanto del emisor como del receptor de la transacción y genera la validación y autorización de la transacción a través de una aplicación, que puede ser una aplicación web progresiva no nativa o una aplicación nativa convencional, en donde el sistema es la parte tangible que permite realizar el método para efectuar una transacción segura, fácil e inmediata mediante el empleo de redes sociales.

La presente invención se relaciona con un sistema y un método para generar una transacción segura por medio de redes sociales mediante la invocación de un comando específico y la implementación de un patrón de seguridad, en donde el método se lleva a cabo en el sistema, en donde el sistema se compone de elementos técnicos tales como un computador, teléfono móvil, tableta, o cualquier otro dispositivo con acceso a internet o similar el cual se pueden encontrar ubicados en diferentes lugares, asimismo esta invención a partir de comandos marcados con etiquetas predefinidas, que toma información necesaria tanto del emisor como del

receptor de la transacción, genera la validación y autorización de la transacción a través de una aplicación, que puede ser una aplicación web progresiva (PWA por sus siglas en inglés) no nativa o una aplicación nativa convencional para validar la identidad del usuario, manteniendo los protocolos de seguridad para garantizar que la transacción sea totalmente segura de acuerdo con los estándares del banco o entidad financiera, esto se lleva a cabo mediante la comunicación entre dispositivos de comunicación electrónicos tales como teléfonos celulares, tablets, computadores, pc portátiles entre otros.

Con base a lo anterior, se tiene como propósito en la presente solicitud de Patente de Invención proteger un sistema (S) y un método (M) para transacciones fáciles y seguras en redes sociales para dispositivos móviles, que se conforma de un conjunto de ordenes o pasos o etapas técnicas (a, b, c, d, e, f, g, 1, 1A, 1B, 1C, 1D, 1E, 1F, 1G, 2 y 2A) que integran el método (M) junto con elementos técnicos (300, 301, 310, 400) que conforman todo el sistema (S), en donde el sistema (S) es la parte tangible que permite realizar el método (M) para efectuar una transacción segura, fácil e inmediata, mediante el empleo de redes sociales (RD). (Ver figuras No.1, No.2, No.3 y No.4).

El sistema (S) y el método (M) para transacciones fáciles y seguras en redes sociales para dispositivos móviles, cuenta con un método (M) que se compone de un conjunto de órdenes, pasos, etapas técnicas o componentes lógicos necesarios para realizar una transacción financiera fácil, segura e inmediata en tiempo real a través de una aplicación de una red social externa a la aplicación bancaria, empleando comandos marcados con etiquetas predefinidas, que toma información necesaria tanto de un emisor como de un receptor de la transacción generando la validación y autorización de la transacción a través de una aplicación, que puede ser una aplicación web progresiva no nativa o una aplicación nativa convencional, esto se hace mediante la integración y la combinación de varios elementos técnicos tangibles que conforman y hacen parte del sistema (S) o (hardware) que junto con el método (M) permiten optimizar la validación de la identidad del usuario, manteniendo todos los protocolos de seguridad que a su vez garantizan que la transacción sea totalmente segura de acuerdo con los estándares del banco o institución financiera, en donde el sistema (S) es la parte tangible que permite realizar el método (M) para efectuar una transacción segura, fácil e inmediata, mediante el empleo de redes sociales; a continuación se expone la secuencia lógica del conjunto de órdenes, pasos o etapas técnicas que integran el método (M) y que a su vez se integra con el sistema (S), la cual se está ilustra de la siguiente manera:

Secuencia lógica de las órdenes, pasos o etapas técnicas que integran el método (M).

Proceso No.1

- a) Ingresar a la aplicación
- b) Iniciar sesión (navegador)
- c) ¿Está registrado?
- d) Si
- e) ¿Agregar Negocio (Red Social)?
- f) Si
- g) Eres vendedor
- h) ¿Vender un producto?
- i) Si
- j) Publicar Producto (Red Social)
- k) Fin
- g) Eres comprador
- h) ¿comprar un producto?
- i) Si
- j) Ingrese a la Red Social
- k) Realizar comentario en el producto del vendedor
- l) ¿Recibir notificación? (Navegador)
- m) No
- n) Activar notificaciones (Navegador)
- o) Iniciar sesión (Navegador)

Proceso No.1A

- a) Ingresar a la aplicación
- b) Iniciar sesión (navegador)
- c) ¿Está registrado?
- d) Si
- e) ¿Agregar Negocio (Red Social)?
- f) Si
- g) Eres vendedor
- h) ¿Vender un producto?
- i) No
- j) Se devuelve a la opción ¿Agregar Negocio (Red Social)?

Proceso No.1C

- a) Ingresar a la aplicación
- b) Iniciar sesión (navegador)
- c) ¿Está registrado?
- d) Si
- e) ¿Agregar Negocio (Red Social)?
- f) No
- g) Eres comprador
- h) ¿comprar un producto?
- i) No
- j) Se devuelve a la opción ¿Agregar Negocio (Red Social)?

Proceso No.1B

- a) Ingresar a la aplicación
- b) Iniciar sesión (navegador)
- c) ¿Está registrado?
- d) Si
- e) ¿Agregar Negocio (Red Social)?
- f) No

Proceso No.1D

- a) Ingresar a la aplicación
- b) Iniciar sesión (navegador)
- c) ¿Está registrado?
- d) Si
- e) ¿Agregar Negocio (Red Social)?
- f) No
- g) Eres comprador
- h) ¿comprar un producto?
- i) Si

- j) Ingrese a la Red Social
- k) Realizar comentario en el producto del vendedor
- l) ¿Recibir notificación? (Navegador)
- m) Autorizar transacción (patrón)
- n) Motor de riesgo ¿Cumple validaciones?
- o) Si
- p) PATRON ¿cumple validaciones?
- q) Si
- r) CORE BANCO ¿cumple validaciones?
- s) Si
- t) Producto comprado (transacción exitosa)
- u) Fin

Proceso No.1E

- a) Ingresar a la aplicación
- b) Iniciar sesión (navegador)
- c) ¿Está registrado?
- d) Si
- e) ¿Agregar Negocio (Red Social)?
- f) No
- g) Eres comprador
- h) ¿comprar un producto?
- i) Si
- j) Ingrese a la Red Social
- k) Realizar comentario en el producto del vendedor
- l) ¿Recibir notificación? (Navegador)
- m) Autorizar transacción (patrón)
- n) Motor de riesgo ¿Cumple validaciones?
- o) No
- p) Producto No comprado (transacción Rechazada)

- q) Se devuelve a Iniciar sesión (navegador)

Proceso No.1F

- a) Ingresar a la aplicación
- b) Iniciar sesión (navegador)
- c) ¿Está registrado?
- d) Si
- e) ¿Agregar Negocio (Red Social)?
- f) No
- g) Eres comprador
- h) ¿comprar un producto?
- i) Si
- j) Ingrese a la Red Social
- k) Realizar comentario en el producto del vendedor
- l) ¿Recibir notificación? (Navegador)
- m) Autorizar transacción (patrón)
- n) Motor de riesgo ¿Cumple validaciones?
- o) Si
- p) PATRON ¿cumple validaciones?
- q) No
- r) Producto No comprado (transacción Rechazada)
- s) Se devuelve a Iniciar sesión (navegador)

Proceso No.1G

- a) Ingresar a la aplicación
- b) Iniciar sesión (navegador)
- c) ¿Está registrado?
- d) Si
- e) ¿Agregar Negocio (Red Social)?
- f) No
- g) Eres comprador
- h) ¿comprar un producto?
- i) Si

- j) Ingrese a la Red Social
- k) Realizar comentario en el producto del vendedor
- l) ¿Recibir notificación? (Navegador)
- m) Autorizar transacción (patrón)
- n) Motor de riesgo ¿Cumple validaciones?
- o) Si
- p) PATRON ¿cumple validaciones?
- q) Si
- r) CORE BANCO ¿cumple validaciones?
- s) No
- t) Producto No comprado (transacción Rechazada)
- u) Se devuelve a Iniciar sesión (navegador)

Proceso No.2

- a) Ingresar a la aplicación
- b) Iniciar sesión (navegador)
- c) ¿Está registrado?
- d) No
- e) ¿Registrarse?
- f) Si
- g) ¿Iniciar sesión con Facebook?
- h) Apertura producto (Core Bancario)
- i) No
- j) Se devuelve a ¿Registrarse?

Proceso No.2A

- a) Ingresar a la aplicación
- b) Iniciar sesión (navegador)
- c) ¿Está registrado?
- d) No
- e) ¿Registrarse?
- f) No
- g) Se devuelve a Iniciar sesión (navegador)

La secuencia lógica del conjunto de órdenes, pasos o etapas técnicas ilustradas anteriormente componen los procesos 1, 1A, 1B, 1C, 1D, 1E, 1F, 1G, 2 y 2A, el cual a su vez estos procesos 1, 1A, 1B, 1C, 1D, 1E, 1F, 1G, 2 y 2A conforman todo el método (M) para realizar una transacción segura, fácil e inmediata, mediante el empleo de redes sociales, el cual se encuentra ilustrado en la figura No.1.

Con base a lo anterior, se ilustra en la figura No.1 cada una de las secuencias lógicas del conjunto de órdenes, pasos o etapas técnicas que conforman los procesos 1, 1A, 1B, 1C, 1D, 1E, 1F, 1G, 2 y 2A, que a su vez conforman todo el método (M) para generar una transacción segura en redes sociales con aplicaciones no nativas o una aplicación nativa convencional en dispositivos móviles (300) de la presente invención, dicho método (M) es ejecutado por un dispositivo electrónico (300, 400) con conexión a internet y que se comunican mediante una red de telecomunicaciones (310), donde dicho dispositivo electrónico (300, 400) se puede encontrar ubicado en algún lugar, este dispositivo electrónico (300, 400) puede corresponder, sin limitación, a un servidor, computador personal, computador portátil, tableta, teléfono móvil, y/o similares que hacen parte del sistema (S). (Ver figuras No.1, No.2, No.3 y No.4).

El método (M) para llevar acabo la secuencia lógica del conjunto de órdenes, pasos o etapas técnicas de los procesos 1, 1A, 1B, 1C, 1D, 1E, 1F, 1G, 2 y 2A comprende cada uno de los siguientes pasos o etapas técnicas que se describirán a continuación y que a su vez también se harán en sincronía mediante la integración y la configuración de varios elementos técnicos (300, 400, 310) que conforman el sistema (S), así:

- a) Registrar (1) y almacenar (1.3, 2.4, 3.1) los datos de un usuario (100) que puede ser un comprador (C) únicamente o un comprador (C) y vendedor (V), en una base de datos de una aplicación web progresiva PWA (200) por sus siglas en inglés, en donde dicho registro (1) incluye la creación de un perfil para cada usuario (100) con los datos personales del mismo, iniciando sesión (2) en una red social (RD) donde se llevará a cabo la transacción y, a su vez, realizará la apertura (1.2) del producto financiero que va a estar relacionado con el usuario (100), en esta etapa de registro y almacenamiento en la base de datos de una aplicación web progresiva PWA (200) se hace mediante un dispositivo móvil (300) que se encuentra conectado a internet y que a su vez se comunica con otro dispositivo electrónico en otro lugar como por ejemplo un servidor o computador (400) conectado a internet. (Ver figura No.2 y No.3).
- b) Asociar el nombre de usuario y datos de sesión de la red social (RD) con los datos del usuario (100), bien sea comprador (C) o vendedor (V), y el ID creado para la PWA (200) que se encuentra en el dispositivo móvil (300) del usuario (100), este paso o etapa se hace mediante la red de telecomunicación (310) entre el dispositivo móvil (300) y el servidor o computador (400) conectado a internet. (Ver figuras No.2 y No.3).
- c) Monitorear y autenticar (1.1) por parte de la red social (RD) en los perfiles de un usuario (100) vendedor (V) y un usuario (100) comprador (C) por medio de un elemento en la arquitectura que permite la interacción entre las redes sociales (RD) y una aplicación transaccional, con el fin de poder determinar cuándo se invoque un comando o etiqueta específica (4) por parte del usuario (100) comprador (C) en la publicación (3) del usuario (100) vendedor (V) para así determinar, cuándo se desea realizar una transacción (compra), este paso o etapa se hace mediante la red de telecomunicación (310) entre el dispositivo móvil (300) y el servidor o computador (400) conectado a internet. (Ver figuras No.2 y No.3).
- d) Validar (6.3) si el usuario (100) que invoca el comando o etiqueta (4) para la realización de la compra se encuentra también asociado a un ID de usuario en la aplicación web progresiva API PWA (200), así como validar si el usuario (100) que recibe el comentario invocando la etiqueta (4) también se encuentra asociado a un ID de usuario vendedor (V), este paso o etapa se hace mediante la red de telecomunicación (310) entre el dispositivo móvil

(300) y el servidor o computador (400) conectado a internet. (Ver figuras No.2 y No.3).

- e) Una vez validada la información del emisor (100) y el receptor (100) en su dispositivo electrónico o móvil (300) (comprador (C) y vendedor (V) respectivamente), se ejecuta la PWA (200) del usuario (100) internamente en dicho dispositivo móvil (300) para que éste autorice la transacción (7.3) mediante un gesto personalizado (7.2') para validación (7.1), solicitando que el usuario (100) comprador (C) introduzca en el dispositivo móvil (300) (específicamente en la aplicación de red social (RD)) un patrón predefinido (7.2'') que sirve para autenticación de la información y comprobación del usuario (100); (Ver figuras No.2 y No.3).
- f) Comparar el patrón (7.2') introducido en el dispositivo móvil (300) con un patrón base (7.2'') almacenado en la base de datos del banco o entidad financiera mediante la comunicación entre el dispositivo móvil (300) y el servidor (400) de la entidad financiera, en donde dicho servidor (400) cuenta con una interfaz de programación de aplicaciones API SP (500) por sus siglas en inglés junto con un motor de riesgo (600), en donde se considera y se tiene en cuenta la velocidad con la que dicho patrón (7.2') fue realizado por el usuario (100) comprador (C); y (Ver figuras No.2 y No.3).
- g) En caso de coincidir ambos patrones (7.2', 7.2''), mediante la comunicación sostenida entre el dispositivo móvil (300) y el servidor (400) del banco o la entidad financiera, realiza la transacción solicitada (7.3) por el usuario (100) comprador (C) y se transfieren los fondos al usuario (100) vendedor (V) de acuerdo con la etiqueta invocada (4) y los valores correspondientes indicados en la publicación de la red social (RD). (Ver figuras No.2 y No.3).

Así las cosas, en una primera etapa del presente método (M), como se ilustra en las figuras No.2 y No.3, se realiza la implementación de una codificación predeterminada de etiquetas (4) y texto para invocar la realización de la transacción, lo cual puede llevarse a cabo a través de un mensaje o comentario en la aplicación de una red social (RD), externa a una aplicación bancaria. Adicionalmente, la invención emplea un servidor (400) que tiene una interfaz de programación de aplicaciones API SP (500) por sus siglas en inglés junto con un motor de riesgo (600) que corresponde a un elemento en la arquitectura que permite la interacción entre las redes sociales (RD) y una aplicación transaccional. (Ver figuras No.1, No.2, No.3 y No.4).

En una modalidad preferida, la aplicación transaccional es una aplicación web progresiva PWA (200) no nativa, que se ejecuta en un dispositivo móvil (300) conectado a internet, dicha aplicación web progresiva PWA (200) no nativa se emplea para la realización de diversas funciones, en donde este tipo de aplicación web progresiva PWA (200) no nativa emplea tecnologías disponibles en los navegadores de dispositivos móviles (300) tal y como se definieron anteriormente,

con el fin de ofrecer una experiencia en los dispositivos móviles (300), muy similar a la de una aplicación nativa, sin tener que ser una aplicación nativa, y en consecuencia, sin tener que realizar una descarga o instalación directamente en el dispositivo móvil (300). Todo esto se realiza en un sistema de telecomunicaciones móviles que permite el acceso a un servidor (400) desde un dispositivo móvil (300), por medio de la red de telecomunicaciones (310), como es evidente para el experto en la materia. (Ver figuras No.2 y No.3).

Así, es importante tener en cuenta que el método (M) anteriormente descrito está condicionado a la publicación (3) de un artículo o producto y/o servicio para venta o similar o la solicitud de dinero y transferencia del mismo en una red social (RD) el cual se hace mediante una aplicación llamada INNVO, dicha aplicación INNVO se encuentra soportada, comunicada y sincronizada mediante la PWA (200) que se encuentra contenida en el dispositivo móvil (300) del usuario (100), dicho usuario (100) mediante la aplicación INNVO puede vincular un perfil, el cual puede ser un perfil de comprador (C) y/o un perfil de vendedor (V), igualmente este usuario (100) puede agregar un emprendimiento o negocio según el perfil que tenga relacionado (comprador (C) y/o vendedor (V) respectivamente). Siguiendo con la descripción, esta aplicación INNVO puede publicar un producto o artículo que ingresa el usuario (100) a esta aplicación INNVO, el cual esta, a su vez publica dicho artículo o producto sobre la red social (RD) haciéndolo de manera automática, sin que dicha aplicación INNVO deba estar necesariamente dentro de la red social (RD), de igual forma esta aplicación INNVO mantiene el registro del inventario de los productos o artículos que el usuario (100) ha publicado y que a su vez le han comprado; esta aplicación INNVO puede iniciar sesión con la red social (RD), asimismo, puede realizar transacciones financieras en redes sociales realizando el proceso de validación mediante patrones (7.2', 7.2'') que, a través de Machine Learning (700) junto con un motor de riesgo (600) que se encuentran contenidos en un servidor (400) realiza capturas de información y datos del usuario (100), luego se verifica de manera segura que dichos patrones (7.2', 7.2'') cumplan con los parámetros establecidos tales como la velocidad y el tiempo para realizar dichos patrones (7.2', 7.2'') perfilando el usuario (100) y a su vez verificándolo para realizar la transacción financiera de manera segura, o al contrario, logrando detectar si hay un posible fraude procediendo a rechazar la transacción financiera. La aplicación INNVO se emplea para comprar artículos, productos o servicios en redes sociales, esto se hace mediante la invocación de un comando o etiqueta específica (4) precedida por un carácter especial, tal como "@InnvoPagar", "INNVO" o cualquier otra que puede ser previamente programada o definida, asimismo, mediante la PWA (200) puede retirar, recargar y transferir dinero a través de cajeros automáticos del banco o alguna entidad financiera e igualmente lo puede hacer desde cualquier cuenta bancaria de ahorros o cuenta corriente que tenga el usuario (100), lo anteriormente descrito, se hace en el presente método (M) junto con el sistema (S) el cual puede reconocer, que se desea hacer una transacción para una transferencia de dinero entre dos usuarios (100) y así, se procede a autorizar (7) o pasar los fondos de una cuenta a otra directamente en la red social (RD), sin necesidad de aplicaciones o elementos adicionales requeridos por un banco o entidad financiera, asimismo, se logra realizar este proceso de manera ágil e inmediato y en tiempo real sin que el

usuario (100) final tenga retrasos considerables. La aplicación INNVO también permite hacer transacciones financieras dentro de un grupo de usuarios (100) de manera segura en la red social (RD) mediante patrones (7.2', 7.2'') sin necesidad de colocar números telefónicos o el ingreso de datos inseguros o que induzcan a algún error, por otro lado, el grupo de usuarios (100) pueden estar vinculados a la aplicación INNVO y a su vez están vinculados a la red social (RD). Esta aplicación INNVO se puede eliminar del dispositivo móvil (300) del usuario (100) de manera fácil sin necesidad de alguna autorización o trámite alguno por parte del banco o entidad financiera. (Ver figuras No.2 y No.3).

Luego, tal como se definió anteriormente, los datos tanto del usuario (100) comprador (C) como del usuario (100) vendedor (V) son registrados (1) y almacenados (1.3, 2.4, 3.1) en la base de datos del PWA (200) que encuentra dentro del dispositivo móvil (300) del usuario (100) (dicho usuario (100) puede ser el mismo, tal como se indicó anteriormente, es decir, un usuario (100) sólo comprador (C) o un usuario (100) comprador (C) y vendedor (V)), donde es posible crear un perfil mediante un registro simplificado (1) que comprende los datos de cada usuario (100), dentro de los que se encuentran: nombres, apellidos, número de celular, correo electrónico, número de documento y su fecha de expedición, donde también es importante tener en cuenta que la información del negocio o emprendimiento (2.1, 2.2) de un usuario (100) vendedor (V) se almacena (2.4, 3.1) en la base de datos del PWA (200) con la información normal del usuario (100) comprador (C) que se encuentra en su dispositivo móvil (300). Todo lo descrito anteriormente, se realiza en la PWA (200) que se halla en el dispositivo móvil (300) del usuario (100). (Ver figuras No.2 y No.3).

Así, una vez se han realizado los respectivos registros en el PWA (200) definidos anteriormente, el usuario (100) debe iniciar sesión con su plataforma de red social (RD) con el objetivo de asociar el ID de su perfil en dicha red con el perfil creado en la PWA (200), y por tanto a su depósito electrónico del producto o cualquier otro producto financiero, tal como, por ejemplo, una cuenta bancaria (ahorros/corriente). De esta manera, cuando el usuario (100) en una red social (RD) desee ejecutar una transacción (7.3), se puede validar (7.1) si existe un perfil de usuario asociado a la cuenta de la PWA (200) para realizar la transacción y ejecutar la aplicación, el proceso anterior, se lleva a cabo mediante la comunicación entre el servidor (400) y el dispositivo móvil (300) del usuario (100). (Ver figuras No.2 y No.3).

Después, una vez un usuario (100), en su condición de comprador (C), indica la voluntad de compra de un producto en la red social (RD) que se encuentra ejecutándose al interior de su dispositivo móvil (300), este usuario (100) invoca la transacción en la publicación del producto mediante un comentario que emplea un conjunto de etiquetas (4) predefinidas, tal como se definió anteriormente, en donde este proceso se desarrolla en su respectivo dispositivo móvil (300). (Ver figuras No.2 y No.3).

De este modo, a partir del ID de red social (RD) del usuario (100) mediante su dispositivo móvil (300) que se comunica con el servidor (400) se comprueba (6.3)

que dicho usuario (100) tenga una cuenta en la PWA (200) asociada y que el receptor (100) de la transacción en la red social (RD) también tenga una cuenta en dicha PWA (200). Así, una vez validada la información del emisor (100) y el receptor (100), se ejecuta la mencionada PWA (200) del usuario (100) en condición de comprador (C) para que este autorice la transacción mediante un gesto personalizado de validación (7.2') que lleva a cabo mediante su dispositivo móvil (300) que se comunica con el servidor (400) de la entidad financiera haciendo que dicho gesto personalizado de validación (7.2') el cual corresponda a un patrón previamente definido (7.2'') y almacenado en el servidor (400) de la entidad financiera. Luego, el patrón (7.2') introducido por el usuario (100) comprador (C) es comparado (6.4) con el patrón base (7.2'') almacenado en la API SP (500) junto con un motor de riesgo (600) que se encuentran en el servidor (400) del banco o entidad financiera, que, en caso de coincidencia de ambos patrones (7.2', 7.2''), la entidad financiera o banco realiza la transacción (7.3) correspondiente y debita el dinero de la cuenta del usuario (100) comprador (C) para pasarlo a la cuenta del usuario (100) vendedor (V), concluyendo así con la compra. (Ver figuras No.2 y No.3).

El gesto personalizado (7.2') es un elemento de la arquitectura del producto cuya función principal es autorizar las transacciones a partir de un gesto predefinido (7.2'') por el usuario (100) que se digita en una ventana generada por la PWA (200) que se lleva a cabo en su respectivo dispositivo móvil (300). Este gesto (7.2') podría desarrollarse, de forma ejemplar pero no limitante, sobre una matriz de puntos 3x3 en la que el usuario (100) puede definir un patrón que no se marca en la pantalla de su dispositivo móvil (300), y la autorización se da por comparación de la totalidad de los puntos, en el mismo orden del gesto predefinido (7.2'') que se encuentra almacenado en la API SP (500) del servidor (400) del banco o entidad financiera. No obstante, la presente invención contempla el uso de cualquier tipo de gesto personalizado (7.2') para la verificación de la identidad del usuario (100) y así autorizar la transacción financiera, donde dicho gesto (7.2') se puede seleccionar, sin limitación, de: matrices de puntos para dibujar un patrón, código de seguridad de varios dígitos (PIN), palabra clave, preguntas de seguridad, etc. (Ver figuras No.2 y No.3).

En una modalidad preferida, la aplicación progresiva PWA (200) que hace parte del método (M) de la presente invención, permite la gestión de inventario de productos o artículos, ofreciendo así enlaces directos con las redes sociales (RD) para realizar publicaciones y actualizar el inventario de los mismos. Adicionalmente, es posible gestionar ambos perfiles del usuario (100) (dicho usuario (100) puede ser el mismo, o un usuario (100) sólo comprador (C) o un usuario (100) comprador (C) y vendedor (V)), dentro de la aplicación web progresiva PWA (200), ofreciendo de esta forma una transaccionalidad entre personas naturales y comercios en las redes sociales (RD). (Ver figuras No.2 y No.3).

En otra modalidad, el método (M) de la presente invención hace uso de inteligencia artificial, concretamente el Machine Learning (700) (aprendizaje de máquina, por su nombre en inglés, el cual será definido más adelante en detalle), tal como se ilustra claramente en la figura No.2, No.3 y No.4, dicho Machine Learning (700) se emplea

con el fin de permitir que la transacción financiera pueda ser realizada de forma más sencilla y rápida de acuerdo con el comportamiento previo de los usuarios (100) y sus transacciones previas, es decir, el sistema (S) asociado al método (M) de la presente invención se conecta con cualquier tipo de sistema de inteligencia artificial que puede ser suministrado por cualquier tipo de proveedor, como se conocen comercialmente, con el fin que dicho sistema (S) sea más eficiente y prediga el comportamiento de los usuarios (100) y la forma como realizan las transacciones para reducir los tiempos de interacción, y demás variables involucradas.

Es importante aclarar que Machine Learning (700), como es claro para el experto en la materia, corresponde a una de las expresiones de la inteligencia artificial en la que la máquina tal como un computador o servidor (400) y/o dispositivo móvil (300) o cualquier maquina tiene capacidades de aprender a realizar tareas, predecir comportamientos y muchas más, a partir del análisis de datos. (Ver figuras No.2, No.3 y No.4).

De acuerdo con lo definido anteriormente sobre el método (M) de la presente invención, es importante tener en cuenta que el empleo de una aplicación web progresiva PWA (200) funciona como el canal transaccional bancario en donde se concentran todas las funcionalidades transaccionales del producto y se gestiona la información de los productos que se publican por parte del usuario (100) en condición de vendedor (V) en redes sociales (RD). La PWA (200) constituye una aplicación web no nativa (INNVO) que incorpora ciertos elementos estándar que posibilitan su funcionamiento en conjunto con la aplicación de la red social (RD), dicha PWA (200) constituye una aplicación web no nativa (INNVO) el cual se puede encontrar en un dispositivo móvil (300) de un usuario (100) que as u vez está conectada por medio de una red de telecomunicaciones (310) a un servidor (400). (Ver figuras No.2, No.3 y No.4).

Uno de esos elementos es una herramienta que impulsa la aparición de la interfaz de usuario de la PWA (200) de manera eficiente y confiable, ya que el código se almacena en la memoria (301) caché del dispositivo móvil (300) del usuario (100) con el que se accede a la red social (RD). (Ver figuras No.2, No.3 y No.4).

Sumado a lo anterior, el método (M) de la presente invención se basa en el empleo del protocolo de seguridad HTTPS en la conexión de internet, el cual garantiza la seguridad de la información financiera entre la PWA (200) y la nube, así como entre la nube y la entidad financiera. Así, la utilización de una aplicación no nativa PWA (200) proporciona ventajas importantes frente a una aplicación nativa, como se definirá a continuación. (Ver figuras No.2, No.3 y No.4).

En primer lugar, dado que la PWA (200) es una aplicación multiplataforma, esta ofrece un diseño de respuesta que se adapta a diferentes tamaños de pantalla de diversos dispositivos móviles (300). Adicional a esto, su empleo garantiza una mayor visibilidad por cuanto la PWA (200) puede aparecer en resultados de búsqueda web y es posible descargarla de manera gratuita, rápida y fácil desde cualquier explorador. Las PWA (200) permiten además generar alertas tipo PUSH (emergentes) para facilitar la comunicación y notificación a los usuarios (100) y

ofrecen rapidez de carga al ejecutarse de manera rápida y eficiente. De esta forma, incorporar lo mejor de las aplicaciones nativas y lo mejor de las páginas web, aunando al hecho que las PWA (200) ocupan un espacio de almacenamiento mínimo respecto a las aplicaciones nativas, el empleo de estas aplicaciones garantizan un mejor desempeño que aquellas aplicaciones nativas existentes en el estado del arte, hecho que permite que el método (M) de la presente invención difiera en gran medida de los existentes en el arte previo.

En una modalidad alterna de la presente invención, la aplicación transaccional utilizada para la realización de la transacción financiera es una aplicación nativa convencional en lugar de una aplicación web progresiva no nativa.

Ahora bien, cuando se hace una referencia del método (M) de la presente invención con respecto a las figuras No.2 y No.3, se tiene que el proceso del pago involucra la interacción de todo el sistema (S), en donde en las figuras No.2 y No.3 ilustran un único usuario (100), que puede crear dos tipos de perfiles: vendedor (V) y comprador (C). Para empezar el proceso, un usuario (100) que quiera tener los perfiles de uso de comprador (C) y vendedor (V), obligatoriamente, debe realizar el registro inicial (1) y agregar o vincular un perfil en su red social (RD) propia de su comercio. (Ver figuras No.1, No.2 y No.3).

De este modo, para que el flujo pueda funcionar, el usuario (100) comprador (C) ingresa a la red social (RD), se registra (1), cuando se registra y en paralelo, se almacena su información (1.3, 2.4, 3.1) de usuario en la base de datos PWA (200). Si decide ser usuario (100) vendedor (V), ingresa a vincular (2.1, 2.2) su emprendimiento o negocio en la red social (RD) y cuando la vincula (2.2), la PWA (200) solicita a la interfaz de programación que almacene el ID del usuario (100) y el ID del usuario (100) vendedor (V), así como del producto o artículo a vender. Para poder realizar este procedimiento, la red social (RD) intenta vincular (5) y validar (6) la página para que sea leída, si la respuesta es exitosa (5, 6), se agrega a la red social (RD) y en paralelo se almacena en la base de datos DB SL (900). Esto implica que en la interfaz de programación ya se tiene un registro como vendedor (V) y que para la red social (RD), dicho usuario (100) vendedor (V) ya es escuchado en dicha página (Ver figura No.2).

Cuando el usuario (100) vendedor (V) aparece registrado como tal en la red social (RD), dicho usuario (100) vendedor (V) puede entonces publicar (3) los productos en la red social (RD) en cuestión, los cuales se van diferenciando por un ID que va asignando la red social (RD) y que se va almacenando (2.3, 6.1, 6.2.1) en la base de datos DB SL (900). (Ver figura No.2).

Una vez pasa esto, un usuario (100) con un perfil de comprador (C), como se ilustra en la figura No.3, dicho usuario (100) comprador (C) ve el producto en la red social (RD) que fue publicado por el usuario (100) vendedor (V) (en el que se evidencia que fue publicado por la PWA (200)). El usuario (100) comprador (C) procede a realizar un comentario en la publicación haciendo uso de los caracteres especiales, como se definieron anteriormente. Luego, como se muestra nuevamente en la figura No.2, la red social (RD) le notifica (5) a la interfaz de programación, quien valida (6) filtrando los comentarios que tienen los caracteres especiales y los deja pasar,

desechando el resto que no son de interés para la transacción. Cuando lo deja pasar, va a la PWA (210) y le entrega (6.2) el ID del producto o artículo, el ID de la página del usuario (100) vendedor (V) y el ID de usuario, para que la PWA (210) valide (6.3) si efectivamente ese usuario (100) (comprador (C)) existe y es usuario de la aplicación bancaria o para transferencia (PWA). Si esto es afirmativo, se devuelve y la interfaz lo registra en su base de datos para guardar información histórica de la transacción de cara a una auditoría. Allí se le notifica desde el navegador de internet (7.4) al usuario (100) comprador (C) toda la información para que pueda comprar el producto en el dispositivo móvil (300). Al abrir la notificación, le aparece toda la información del producto y al verificar que está bien, el usuario (100) comprador (C) acepta y aparece el patrón (7.2'), mostrado en la Figura No.2 (método para autorizar las transacciones), allí, el usuario (100) comprador (C) dibuja el patrón (7.2') o ingresa la información de verificación, inmediatamente se invoca al patrón base (7.2'') que se encuentra almacenado en la API SP (500) (donde se captura la velocidad en que se realiza, los puntos seleccionados y la secuencia de los mismos), lo cual es reenviado (7.2') hacia la PWA (200) del dispositivo móvil (300) (nótese que la figura No.2 indica una flecha para este proceso de doble vía), quien el patrón base (7.2'') que se encuentra almacenado en la API SP (500) junto con un motor de riesgo (600), es el encargado de indicar si efectivamente es el usuario (100) comprador (C) identificado. (Ver figuras No.2 y No.3).

Adicionalmente, aquí entra en funcionamiento un motor de riesgo (600), mostrado en la figuras No.2, No.3 y No.4, donde en el motor de riesgo (600) perfila al cliente o usuario (100) con relación a si es apto o no para hacer una transacción, es decir, si cumple con las condiciones preestablecidas para poder llevar a cabo una transacción de compra en una red social (RD).

Cuando se pasa las etapas de validación del patrón (7.2'), el motor de riesgo (600), procede a realizar la transacción en el núcleo bancario (1000) o entorno de la entidad financiera, donde se valida que haya saldo en la cuenta bancaria, que haya aún productos disponibles y otras cuestiones de ley. Luego de concretar la venta, la PWA (200) le notifica (7.4) al usuario (100) vendedor (V) que le compraron su producto publicado en la red social (RD). (Ver figura No.2).

El motor de riesgo (600) que se emplea para verificar y validar al cliente o usuario (100) para saber si es apto o no, para hacer una transacción, cumpliendo con las condiciones preestablecidas por el banco o entidad financiera con el fin de llevar a cabo una transacción segura de compra en una red social (RD), dicho proceso se hace mediante la configuración y disposición de varios elementos que junto con unos pasos o etapas que se llevan a cabo dentro del motor de riesgo (600) se hace de la siguiente manera: desde la PWA (200) que se encuentra en el dispositivo móvil (300) del usuario (100), dicho usuario (100) envía (1) el gesto personalizado (7.2') para la verificación de su identidad con el fin de autorizar la transacción financiera, dicho gesto (7.2') es un conjunto de datos de información que se va a verificar y comparar frente a un patrón base (7.2'') que se encuentra almacenado en la API SP (500), para hacer este proceso se envía este gesto (7.2') mediante un conjunto de datos de información que se envían al elemento llamado Event Hub (1000) o core

bancario (el Event Hub (1000) o core bancario puede llamar o traer datos de una base de datos externa de un servidor (400) de la entidad financiera o banco) para gestionar la información que a su vez la envía (2) al elemento llamado Stream Analytics – Real time (920) el cual realiza el análisis y la comparación de la información, cuando esta información cumple (4) se envía al elemento llamado Data Factory (930) el cual organiza la información y la almacena (5) en el elemento llamado DB- Fraud Deteccion Results SQL (910), asimismo esta información también se envía (5.1) al Machine Learning engine (700) donde este a su vez procesa la información y responde (5.2), mediante la información allegada al machine learning engine (700) donde se envía nuevamente la información al elemento llamado DB-Fraud Deteccion Results SQL (910), asimismo si la información enviada desde el elemento llamado Event Hub (1000) o core bancario para gestionar la información que a su vez la envía (2) al elemento llamado Stream Analytics – Real time (920) el cual realiza el análisis y comparación de la información y cuando esta información no cumple (3) se almacena en el elemento llamado DB-Fraud Deteccion Results SQL (910), después de que la información ha pasado por el elemento llamado DB- Fraud Deteccion Results SQL (910) se realiza su validación en donde puede ser rechazada (3.1), aceptada (5.3) rechazada/ aceptada (6.2) a la PWA (200) que encuentra en el dispositivo móvil (300) del usuario (100), asimismo esta información se puede enviar desde el elemento llamado DB- Fraud Deteccion Results SQL (910) para realizar una segunda validación (6) a una base de datos DB SL (900) de un servidor (400) para validar (6.1) la información como medida de seguridad para estar seguros de poder realizar la transacción. El machine learning engine (700) que se encuentra en el motor de riesgo (600) puede procesar y aprender de la información allegada y recibida (5.4) de la PWA (200) que se encuentra en el dispositivo móvil (300) del usuario (100) y también de la información allegada o recibida de un servidor (400) que se encuentra en otro lugar. (Ver figura No.4).

La presente invención cuenta con un sistema (S) para llevar a cabo el método (M) como se definió anteriormente, en donde dicho sistema (S) está conformado por un dispositivo móvil (300) de un primer usuario (100) (comprador (C) /vendedor (V)) que cuenta con una aplicación para el acceso a una red social (RD) y que además permite acceder a internet, en donde dicho dispositivo (300) además incluye una memoria interna (301) para el almacenamiento de los datos de usuario para poder ingresar a la hora de acceder a la red social (RD) mediante la aplicación incluida (INNVO); una red de telecomunicaciones (310) que permita realizar la conexión de múltiples dispositivos móviles (300) con internet y con una red social (RD) para acceso; un servidor (400) donde se almacena la red social (RD) y permite tener acceso a los usuarios (100) de la misma, donde dicho servidor (400) puede ser de tipo tangible o virtual ubicado en una nube o en un computador ubicado en otro lugar, en donde el servidor (400) se comunica con los dispositivos móviles (300) por medio de la red de comunicaciones (310) e internet; un servidor seguro (400) de transacciones, el cual es de propiedad de la entidad financiera y que se conecta por medio de la red de telecomunicaciones (310) con los demás dispositivos móviles (300); y un segundo dispositivo móvil (300) correspondiente a un segundo usuario (100) (comprador (C) /vendedor (V)) que se comunica con los demás elementos o

componentes del sistema (S) mediante la red de telecomunicaciones (310), en donde dicho segundo dispositivo móvil (300) también cuenta con la aplicación para acceso a la red social (RD) por parte del segundo usuario (100). (Ver figuras No.2, No.3 y No.4).

Así las cosas, el sistema (S) de la presente invención es utilizado para realizar una transacción segura mediante una red social (RD), donde dicha transacción se realiza entre dos usuarios (100) configurados como comprador (C) y vendedor (V), respectivamente, donde uno de dichos usuarios (100) publica un producto (3) o un servicio que ofrece en venta mientras que el segundo usuario (100) configurado como comprador (C) realiza la compra mediante la red social (RD) utilizando una serie de etiquetas (4) que son reconocidas por la red social (RD) y así se realiza la transacción (7.3) de una forma segura y siguiendo unos patrones (7.2', 7.2'') de validación, con el fin de realizar la comunicación con el servidor (400) del core bancario (1000) (entidad financiera) y así, poder realizar la transferencia de fondos desde la cuenta del usuario (100) comprador (C) a la del usuario (100) vendedor (V), informando de esta forma a los dos usuarios (100) que la transacción fue realizada de forma exitosa. La transacción segura se realiza mediante el método (M) anteriormente ilustrado, el cual permite obtener como resultado dicha transacción de forma segura entre dos usuarios (100) que se configuran como vendedor (V) y comprador (C). (Ver figuras No.1, No.2, No.3, No.4).

En la presente solicitud, se emplea el término “dispositivo móvil” (300) a cualquier dispositivo electrónico que pueda acceder a una red, tal como internet, por cualquier medio, con el fin de poder acceder de la misma forma a una red social (RD), en donde dicho dispositivo móvil (300) puede ser seleccionado, sin limitación, del grupo que consiste de un teléfono móvil, un computador portátil, un computador de escritorio, un servidor, un asistente personal, una tableta, o similar. (Ver figuras No.2, No.3, No.4).

En la presente solicitud, se emplea el término “etiqueta” (4) a una expresión o palabra que permite resaltar un comentario que se puede realizar en la red social (RD), en donde dicha etiqueta (4) puede ser cualquier término o expresión sin limitación, la cual preferiblemente puede ser antecedida por algún elemento adicional, tal como un signo adicional predefinido o algún símbolo ortográfico u otro. (Ver figura No.4).

En la presente solicitud, se emplea el término “gesto personalizado” (7.2') a una expresión que permite realizar la validación de una transacción, en donde dicho “gesto personalizado” (7.2') no tiene ninguna limitación y puede ser usado cualquier medio que permita realizar la validación de la identidad del usuario (100) comprador (C) o vendedor (V) y puede ser seleccionado, sin limitación, de un número de seguridad (PIN), un patrón de dibujo, un menú desplegable, unas preguntas de seguridad, o similares, entre otros. (Ver figuras No.2, No.3, No.4).

En la presente solicitud, se emplea el término “Machine Learning” (700) el cual hace referencia al proceso de inteligencia artificial que permite que una máquina tal como

un computador o servidor (400) y/o dispositivo móvil (300) u otro, pueda aprender a tomar decisiones de forma adecuada dependiendo de un patrón (7.2', 7.2'') o secuencia de acciones previas notadas por dicha máquina, con el fin de acelerar el proceso de toma de decisiones futuras. (Ver figuras No.2, No.3, No.4).

BREVE DESCRIPCIÓN DE LAS FIGURAS:

Figura No.1. Muestra un diagrama de flujo que expone la secuencia lógica del conjunto de órdenes, pasos o etapas técnicas que integran el método (M) y que a su vez se integra con el sistema (S) para transacciones fáciles y seguras en redes sociales para dispositivos móviles de la presente invención.

Figura No.2. Muestra un diagrama general que expone todos los elementos técnicos tangibles e intangibles junto con su respectiva interacción que forman parte y que juegan un papel importante en el sistema (S) y el método (M) para transacciones fáciles y seguras en redes sociales para dispositivos móviles de la presente invención.

Figura No.3. Muestra un diagrama del proceso funcional de la aplicación con configuración cuando el usuario (100) se encuentra bajo el perfil de comprador (C) para la realización de una transacción segura, asimismo en esta figura No.3 se ilustra el diagrama con todos los elementos técnicos tangibles e intangibles junto con su respectiva interacción y que a su vez forma parte del sistema (S) y el método (M) para transacciones fáciles y seguras en redes sociales para dispositivos móviles de la presente invención.

Figura No.4. Muestra un diagrama del proceso funcional del motor de riesgo (600) junto con todos sus elementos técnicos tangibles e intangibles y su respectiva interacción que se lleva a cabo dentro del método (M) y el sistema (S) para transacciones fáciles y seguras en redes sociales para dispositivos móviles de la presente invención.

REIVINDICACIONES

1. Un sistema y un método para transacciones fáciles y seguras en redes sociales para dispositivos móviles, que comprende un método que se **caracteriza porque** comprende las siguientes pasos o etapas técnicas:
 - a) Registrar (1) y almacenar (1.3, 2.4, 3.1) los datos de un usuario (100) que puede ser un comprador (C) únicamente o un comprador (C) y vendedor (V), en una base de datos de una aplicación web progresiva PWA (200) por sus siglas en inglés, en donde dicho registro (1) incluye la creación de un perfil para cada usuario (100) con los datos personales del mismo, iniciando sesión (2) en una red social (RD) donde se llevará a cabo la transacción y, a su vez, realizará la apertura (1.2) del producto financiero que va a estar relacionado con el usuario (100), en esta etapa de registro y almacenamiento en la base de datos de una aplicación web progresiva PWA (200) se hace mediante un dispositivo móvil (300) que se encuentra conectado a internet y que a su vez se comunica con otro dispositivo electrónico en otro lugar como por ejemplo un servidor o computador (400) conectado a internet.
 - b) Asociar el nombre de usuario y datos de sesión de la red social (RD) con los datos del usuario (100), bien sea comprador (C) o vendedor (V), y el ID creado para la PWA (200) que se encuentra en el dispositivo móvil (300) del usuario (100), este paso o etapa se hace mediante la red de telecomunicación (310) entre el dispositivo móvil (300) y el servidor o computador (400) conectado a internet.
 - c) Monitorear y autenticar (1.1) por parte de la red social (RD) en los perfiles de un usuario (100) vendedor (V) y un usuario (100) comprador (C) por medio de un elemento en la arquitectura que permite la interacción entre las redes sociales (RD) y una aplicación transaccional, con el fin de poder determinar cuándo se invoque un comando o etiqueta específica (4) por parte del usuario (100) comprador (C) en la publicación (3) del usuario (100) vendedor (V) para así determinar, cuándo se desea realizar una transacción (compra), este paso o etapa se hace mediante la red de telecomunicación (310) entre el dispositivo móvil (300) y el servidor o computador (400) conectado a internet.
 - d) Validar (6.3) si el usuario (100) que invoca el comando o etiqueta (4) para la realización de la compra se encuentra también asociado a un ID de usuario en la aplicación web progresiva API PWA (200), así como validar si el usuario (100) que recibe el comentario invocando la etiqueta (4) también se encuentra asociado a un ID de usuario vendedor (V), este paso o etapa se hace mediante la red de telecomunicación (310) entre el

dispositivo móvil (300) y el servidor o computador (400) conectado a internet.

- e) Una vez validada la información del emisor (100) y el receptor (100) en su dispositivo electrónico o móvil (300) (comprador (C) y vendedor (V) respectivamente), se ejecuta la PWA (200) del usuario (100) internamente en dicho dispositivo móvil (300) para que éste autorice la transacción (7.3) mediante un gesto personalizado (7.2') para validación (7.1), solicitando que el usuario (100) comprador (C) introduzca en el dispositivo móvil (300) (específicamente en la aplicación de red social (RD)) un patrón predefinido (7.2'') que sirve para autenticación de la información y comprobación del usuario (100).
 - f) Comparar el patrón (7.2') introducido en el dispositivo móvil (300) con un patrón base (7.2'') almacenado en la base de datos del banco o entidad financiera mediante la comunicación entre el dispositivo móvil (300) y el servidor (400) de la entidad financiera, en donde dicho servidor (400) cuenta con una interfaz de programación de aplicaciones API SP (500) por sus siglas en inglés junto con un motor de riesgo (600), en donde se considera y se tiene en cuenta la velocidad con la que dicho patrón (7.2') fue realizado por el usuario (100) comprador (C).
2. Un sistema y un método para transacciones fáciles y seguras en redes sociales para dispositivos móviles, que comprende un método, según la reivindicación No.1, **caracterizada porque** la aplicación transaccional es una aplicación web progresiva PWA (200) no nativa.
 3. Un sistema y un método para transacciones fáciles y seguras en redes sociales para dispositivos móviles, que comprende un método, según la reivindicación No.1, **caracterizada porque** la aplicación transaccional es una aplicación nativa.
 4. Un sistema y un método para transacciones fáciles y seguras en redes sociales para dispositivos móviles, que comprende un método, según la reivindicación No.1, **caracterizada porque** el conjunto de etiquetas distintivas incluye la etiqueta (4) @InnvoPagar y la etiqueta INNVO.
 5. Un sistema y un método para transacciones fáciles y seguras en redes sociales para dispositivos móviles, que comprende un método, según la reivindicación No.1, **caracterizada porque** en donde los datos de cada usuario en el registro son nombres, apellidos, número de celular, correo electrónico, número de documento y su fecha de expedición.
 6. Un sistema y un método para transacciones fáciles y seguras en redes sociales para dispositivos móviles, que comprende un método, según la reivindicación No.1, **caracterizada porque** el gesto personalizado (7.2') se

selecciona de matrices de puntos para dibujar un patrón, código de seguridad de varios dígitos (PIN), palabra clave, o preguntas de seguridad.

7. Un sistema y un método para transacciones fáciles y seguras en redes sociales para dispositivos móviles, que comprende un método, según la reivindicación No.1, **caracterizada porque** realiza transacciones financieras mediante patrones (7.2', 7.2'') que a través de un machine learning (700) junto con un motor de riesgo (600) que se encuentran contenidos en un servidor (400) realiza capturas de información y datos del usuario (100) el cual se verifica de manera segura que dichos patrones (7.2', 7.2'') cumplan con los parámetros establecidos tales como la velocidad y el tiempo para realizar dichos patrones (7.2', 7.2'') perfilando el usuario (100) y a su vez verificándolo para realizar la transacción financiera de manera segura, o al contrario, logrando detectar si hay un posible fraude procediendo a rechazar la transacción financiera.
8. Un sistema y un método para transacciones fáciles y seguras en redes sociales para dispositivos móviles, que comprende un método, según la reivindicación No.1, **caracterizada porque** la aplicación progresiva PWA permite la gestión de inventario de productos o artículos, ofreciendo así enlaces directos con las redes sociales (RD) para realizar publicaciones y actualizar el inventario de los mismos.
9. Un sistema y un método para transacciones fáciles y seguras en redes sociales para dispositivos móviles, que comprende un método, según la reivindicación No.1, **caracterizada porque** la aplicación progresiva PWA (200) permite gestionar ambos perfiles del usuario (100) (dicho usuario (100) puede ser el mismo, o un usuario (100) sólo comprador (C) o un usuario (100) comprador (C) y vendedor (V)), ofreciendo de esta forma una transaccionalidad entre personas naturales y comercios en las redes sociales (RD).
10. Un sistema y un método para transacciones fáciles y seguras en redes sociales para dispositivos móviles, que comprende un método, según la reivindicación No.1, **caracterizada porque** comprende un machine learning (700) que permite que la transacción financiera pueda ser realizada de forma más sencilla y rápida de acuerdo con el comportamiento previo de los usuarios (100).
11. Un sistema y un método para transacciones fáciles y seguras en redes sociales para dispositivos móviles, que comprende un método, según la reivindicación No.1, **caracterizada porque** comprende el protocolo de seguridad HTTPS en la conexión de internet, el cual garantiza la seguridad de la información financiera entre la PWA (200) y la nube, así como entre la nube y la entidad financiera.

12. Un sistema y un método para transacciones fáciles y seguras en redes sociales para dispositivos móviles, que comprende un método, según la reivindicación No.1, **caracterizada porque** comprende un motor de riesgo (600) para verificar y validar al cliente o usuario (100) para saber si es apto o no, para hacer una transacción, cumpliendo con las condiciones preestablecidas por el banco o entidad financiera con el fin de llevar a cabo una transacción segura de compra en una red social (RD).
13. Un sistema y un método para transacciones fáciles y seguras en redes sociales para dispositivos móviles, que comprende un método, según la reivindicación No.1, **caracterizada porque** comprende un motor de riesgo (600) que comprende los siguientes elementos: un elemento Event Hub (1000) o core bancario, un elemento Stream Analytics – Real time (920), un elemento Data Factory (930), un elemento machine learning engine (700) y un elemento DB-Fraud Deteccion Results SQL (910).
14. Un sistema y un método para transacciones fáciles y seguras en redes sociales para dispositivos móviles, que comprende un método, según la reivindicación No.1, **caracterizada porque** comprende un motor de riesgo (600) que comprende unos pasos o etapas: Desde la PWA (200) que se encuentra en el dispositivo móvil (300) del usuario (100), dicho usuario (100) envía (1) el gesto personalizado (7.2') para la verificación de su identidad con el fin de autorizar la transacción financiera, dicho gesto (7.2') es un conjunto de datos de información que se va a verificar y comparar frente a un patrón base (7.2'') que se encuentra almacenado en la API SP (500), para hacer este proceso se envía este gesto (7.2') mediante un conjunto de datos de información que se envían al elemento llamado Event Hub (1000) o core bancario (el Event Hub (1000) o core bancario puede llamar o traer datos de una base de datos externa de un servidor (400) de la entidad financiera o banco) para gestionar la información que a su vez la envía (2) al elemento llamado Stream Analytics – Real time (920) el cual realiza el análisis y la comparación de la información, cuando esta información cumple (4) se envía al elemento llamado Data Factory (930) el cual organiza la información y la almacena (5) en el elemento llamado DB- Fraud Deteccion Results SQL (910), asimismo esta información también se envía (5.1) al machine learning engine (700) donde este a su vez procesa la información y responde (5.2), mediante la información allegada al machine learning engine (700) donde se envía nuevamente la información al elemento llamado DB-Fraud Deteccion Results SQL (910), asimismo si la información enviada desde el elemento llamado Event Hub (1000) o core bancario para gestionar la información que a su vez la envía (2) al elemento llamado Stream Analytics – Real time (920) el cual realiza el análisis y comparación de la información y cuando esta información no cumple (3) se almacena en el elemento llamado DB- Fraud Deteccion Results SQL (910), después de que la información ha pasado por el elemento llamado DB- Fraud Deteccion Results SQL (910) se realiza su validación en donde puede ser rechazada (3.1), aceptada (5.3) rechazada/ aceptada (6.2) a la PWA (200) que encuentra en el dispositivo móvil (300)

del usuario (100), asimismo esta información se puede enviar desde el elemento llamado DB- Fraud Deteccion Results SQL (910) para realizar una segunda validación (6) a una base de datos DB SL (900) de un servidor (400) para validar (6.1) la información como medida de seguridad para estar seguros de poder realizar la transacción. El machine learning engine (700) que se encuentra en el motor de riesgo (600) puede procesar y aprender de la información allegada y recibida (5.4) de la PWA (200) que se encuentra en el dispositivo móvil (300) del usuario (100) y también de la información allegada o recibida de un servidor (400) que se encuentra en otro lugar.

15. Un sistema y un método para transacciones fáciles y seguras en redes sociales para dispositivos móviles, que comprende un sistema que se **caracteriza porque** contiene los siguientes elementos técnicos:

- a. Un dispositivo móvil (300) que tiene una aplicación para el acceso a una red social (RD) y que además permite acceder a una red internet, además incluye una memoria interna (301) para el almacenamiento de los datos de un usuario para poder ingresar a la red social (RD) mediante una aplicación incluida.
- b. Una red de telecomunicaciones (310) que permite realizar la conexión de múltiples dispositivos móviles (300) a través de una red de internet.
- c. Un servidor (400) que almacena una red social (RD) permite tener acceso a los usuarios (100) de la misma, donde dicho servidor (400) puede ser de tipo tangible o virtual ubicado en una nube o en un computador ubicado en otro lugar, en donde el servidor (400) se comunica con los dispositivos móviles (300) por medio de la red de comunicaciones (310).
- d. Un servidor seguro (400) de entidad financiera que se conecta por medio de la red de telecomunicaciones (310) con los demás dispositivos móviles (300).
- e. Un segundo dispositivo móvil (300) correspondiente a un segundo usuario (100) (comprador (C) /vendedor (V)) que se comunica con los demás elementos o componentes del sistema (S) mediante la red de telecomunicaciones (310), en donde dicho segundo dispositivo móvil (300) también cuenta con la aplicación para acceso a la red social (RD) por parte del segundo usuario (100), además incluye una memoria interna (301) para el almacenamiento de los datos del usuario..