

NUEVO CAPITULO REIVINDICATORIO

1. Un método para transacciones fáciles y seguras en redes sociales para dispositivos móviles **caracterizado porque** comprende:

5

- 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.

10

- Una red de telecomunicaciones (310) que permite realizar la conexión de múltiples dispositivos móviles (300) a través de una red de internet.

15

- Un servidor (400) que almacena una red social (RD) permite tener acceso a los usuarios (100) de la misma.

20

- Un servidor seguro (400) de entidad financiera que se conecta por medio de la red de telecomunicaciones (310) con los demás dispositivos móviles (300).

El método comprende los siguientes pasos o etapas técnicas:

25

- 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

35

se comunica con otro dispositivo electrónico en otro lugar como por ejemplo un servidor o computador (400) conectado a internet.).

- 5 **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
- 10 telecomunicación (310) entre el dispositivo móvil (300) y el servidor o computador (400) conectado a internet.
- 15 **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
- 20 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
- 25 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.
- 30 **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
- 35 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).

g) 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).

h) Enviar 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.

- 5 **i)** Enviar (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).
- 10 **j)** Enviar (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).
- 15 **k)** Enviar 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.
- 20 **l)** Enviar (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).
- 25 **m)** Validar 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).
- 30 **n)** 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).
- 35 **o)** Validar (6.1) la información como medida de seguridad para estar seguros de poder realizar la transacción.
- p)** 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.

5

2. Un método de acuerdo con 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).

10

3. Un método de acuerdo con la reivindicación No.1, **caracterizada porque** este dispositivo electrónico (300, 400) puede corresponder, sin limitación, a un servidor, computador personal, computador portátil, tableta, teléfono móvil.

15

4. Un método de acuerdo con la reivindicación No.1, **caracterizada porque** el servidor (310) 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).

20

5. Un método de acuerdo con la reivindicación No.1, **caracterizada porque** Un dispositivo móvil (300) 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.

25

6. Un sistema para transacciones fáciles y seguras en redes sociales para dispositivos móviles **caracterizado porque** comprende:

30

- 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.

35

- Una red de telecomunicaciones (310) que permite realizar la conexión de múltiples dispositivos móviles (300) a través de una red de internet.

5 • Un servidor (400) que almacena una red social (RD) permite tener acceso a los usuarios (100) de la misma.

10 • Un servidor seguro (400) de entidad financiera que se conecta por medio de la red de telecomunicaciones (310) con los demás dispositivos móviles (300).

En donde el dispositivo de procesamiento electrónico (300) que contiene un aplicativo móvil, el cual está configurado para:

15 **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.).

30 **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.

35

- 5 **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
- 10 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.
- 15 **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)
- 20 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.
- 25 **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
- 30 (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
- 35 comprobación del usuario (100).

- 5 **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).
- 10
- 15 **g)** 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).
- 20 **h)** Enviar 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
- 25 gestionar la información.
- 30 **i)** Enviar (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).
- 35 **j)** Enviar (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).

k) Enviar 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.

5

l) Enviar (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).

10

m) Validar 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).

15

n) 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).

20

o) Validar (6.1) la información como medida de seguridad para estar seguros de poder realizar la transacción.

p) 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.

25

30

7. Un sistema de acuerdo con 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

35

engine (700) y un elemento DB-Fraud Deteccion Results SQL (910).

5 **8.** Un sistema de acuerdo con la reivindicación No.1, **caracterizada porque** este dispositivo electrónico (300, 400) puede corresponder, sin limitación, a un servidor, computador personal, computador portátil, tableta, teléfono móvil.

10 **9.** Un sistema de acuerdo con la reivindicación No.1, **caracterizada porque** el servidor (310) 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).

15 **10.** Un sistema de acuerdo con la reivindicación No.1, **caracterizada porque** Un dispositivo móvil (300) 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.

20