

MÉTODO Y SISTEMA PARA EL CONTROL REMOTO DEL ACCESO A ELECTRODOMÉSTICOS

CONTEXTO

Los dispositivos para usuarios como productos electrónicos y electrodomésticos suelen venderse como una compra de pago único por adelantado. Por ejemplo, un televisor podría venderse en una tienda minorista por \$200 al cliente, quien pasa a ser dueño de este y se lo lleva a su hogar. Sin embargo, algunas personas preferirían pagar por un dispositivo en el transcurso del tiempo, por ejemplo, con pagos mensuales de \$20, ya sea por una cantidad limitada de pagos, o mientras se utilice el dispositivo.

Existen diversos sistemas para ayudar al vendedor a seguir recibiendo pagos luego de que el comprado se ha marchado con el televisor (u otro dispositivo o electrodoméstico). En un sistema anterior, múltiples unidades de equipos deben estar conectadas al dispositivo (o a múltiples dispositivos), incluida una unidad para controlar el dispositivo, y otra para gestionar el uso (p. ej., recibir y hacer un seguimiento de los pagos). Por otro lado, otros sistemas usan una red de comunicación móvil que posibilita la verificación de pagos electrónicos. No obstante, estos sistemas también requieren que el dispositivo en sí tenga la función de comunicación móvil para ser controlado.

Conviene tener un método y sistema de control remoto de los dispositivos que sea fácil y rentable de implementar, y que ayude a garantizar que los pagos necesarios se realicen de forma oportuna al vendedor de los dispositivos.

BREVE DESCRIPCIÓN DE LOS ESQUEMAS

La **Figura 1** es un diagrama de bloques de un sistema de control remoto del dispositivo de acuerdo con una un diseño.

La **Figura 2** es un diagrama de bloques de un sistema de control remoto del dispositivo de acuerdo con una un diseño.

La **Figura 3** es un diagrama de flujo de un método de control remoto del dispositivo de acuerdo con un diseño.

La **Figura 4** es un diagrama de bloques de un sistema en el cual se está controlando el electrodoméstico, e ilustra un método para prevenir la manipulación del software de control en el teléfono móvil.

La **Figura 5** es un diagrama de bloques de un sistema en el cual se está controlando el electrodoméstico, e ilustra un método para prevenir la manipulación del software de control en el teléfono móvil.

La **Figura 6** es un diagrama de bloques de un sistema en el cual se está controlando el electrodoméstico, e ilustra un método para prevenir la manipulación del software de control en el teléfono móvil.

La **Figura 7** es un diagrama de bloques de un sistema en el cual se está controlando el electrodoméstico, e ilustra un método para prevenir la manipulación del software de control en el teléfono móvil.

La **Figura 8** es un diagrama de bloques de un sistema en el cual se está controlando el electrodoméstico, e ilustra un método para prevenir la manipulación del software de control en el teléfono móvil.

La **Figura 9** es un diagrama de bloques en el que se ilustra un diseño que permite la financiación para usuarios de teléfonos móviles.

La **Figura 10** es una captura de pantalla en la que se muestra una funcionalidad de un diseño.

La **Figura 11** es una captura de pantalla en la que se muestra una funcionalidad de un diseño.

La **Figura 12** es una captura de pantalla en la que se muestra una funcionalidad de un diseño.

La **Figura 13** es una captura de pantalla en la que se muestra una funcionalidad de un diseño.

La **Figura 14** es una captura de pantalla en la que se muestra una funcionalidad de un diseño.

La **Figura 15** es una captura de pantalla en la que se muestra una funcionalidad de un diseño.

La **Figura 16** es una captura de pantalla en la que se muestra una funcionalidad de un diseño.

DESCRIPCIÓN DETALLADA

Entre los diseños aquí detallados se incluye un sistema que ejecuta método de control remoto de dispositivos o electrodomésticos. Según se usa aquí, "electrodoméstico" significa cualquier dispositivo electrónico que podría comprar habitualmente un usuario. Entre los electrodomésticos se incluyen, entre otros: televisor, refrigerador, congelador, lavadora de ropa, lavadora de platos, horno eléctrico, microondas, licuadora, procesador de alimentos, aire acondicionado, sistema de estéreo, cámara, grabadora de video, teléfono móvil, computadora portátil, computadora de escritorio, tablet, impresora, reproductor de DVD, proyector de video, motocicleta, automóvil o avión.

A los fines de describir los diseños que se reivindican, se brinda un ejemplo de control, activación o desactivación de un electrodoméstico en función de si se realiza pagos mensuales. Pero este es un solo ejemplo de la necesidad de un tercero (como entidad de pago que gestiona cuentas en nombre del vendedor del dispositivo para usuarios) controlar fácilmente y de forma remota el acceso al electrodoméstico por parte del usuario, o incluso la forma en que lo usa.

Los diseños de la invención posibilitan al usuario a poseer y usar un dispositivo o electrodoméstico mientras un tercero puede controlar el uso que se hace de este, lo cual incluye que el tercero determine cuándo puede encenderse el dispositivo, o estar disponible para su encendido. Esto incluye, además, que el tercero determine cómo puede usarse el dispositivo, por ejemplo, qué canales puede recibir un televisor o cuánta potencia puede producir un generador.

La **Figura 1** es un diagrama de bloques de un diseño de un sistema para el control remoto del acceso a electrodomésticos para usuarios. Un electrodoméstico 104 se activa o desactiva mediante un sistema de control de electrodomésticos AMS 101. En un diseño el AMS es un subsistema de equipo integrado en el electrodoméstico, como un microcontrolador o cualquier tipo de circuito integrado (CI). En dicho diseño, el AMS 101 puede integrarse en el centro del electrodoméstico para que no pueda quitarse el sistema

integrado sin inhabilitar el electrodoméstico. Cuando el AMS 101 determina que el cliente ha pagado, habilita el electrodoméstico para su uso normal. En otros diseños, el AMS 101 se conecta luego de la fabricación del electrodoméstico y no está integrado. No obstante, la extracción del AMS 101 es detectable, y lleva a la inhabilitación del electrodoméstico.

En un diseño, el sistema integrado no tiene capacidad de comunicación por sí mismo a excepción de un puerto USB estándar 105, mediante el cual se puede conectar a un dispositivo con funcionalidad para Internet 106, a través de un cable USB 107. En otros diseños, diferentes modos de comunicación, que se sabe que permiten el intercambio de datos con entidades, se encuentran dentro del alcance de la invención. En un diseño, el dispositivo 106 es un teléfono móvil que ejecuta una aplicación de software 102 que habilita al dispositivo 106 a comunicarse con el AMS 101 de acuerdo con los métodos aquí descritos. En otros diseños, el dispositivo con funcionalidad para Internet es una computadora portátil, una computadora personal, una tablet, una agenda electrónica (PDA) o cualquier otro dispositivo de este estilo.

De acuerdo con un diseño, el dispositivo 106 es un teléfono móvil que actúa como un dispositivo de almacenamiento USB. En este caso, tanto la aplicación de software 102 como el sistema integrado pueden comunicarse entre sí al leer y escribir archivos en un dispositivo de almacenamiento USB. En funcionamiento, el AMS 101 le comunica una identificación de electrodoméstico (p. ej., un número de serie) 114 a la aplicación del software 102. Cuando la aplicación del software 102 determina que se realizó un pago por el electrodoméstico identificado, esta aplicación de software 102 entrega un comprobante de pago digital 109 con una firma digital 110 al AMS 101, y el AMS 101 activa el electrodoméstico.

En un diseño, la aplicación del software 102 se comunica mediante un sistema de comunicación por teléfono móvil, que puede usar Wi-Fi 802.11 para comunicarse con un punto de acceso Wi-Fi 111, o puede usar una red de datos móviles GSM como 4G LTE, 3G o 2G EDGE para comunicarse con una torre de señal de una compañía móvil 108. Ya sea mediante Wi-Fi o datos móviles, el teléfono transmite datos por Internet a una

infraestructura de terceros 103 que incluye por lo menos un servidor de control de dispositivo remoto (RDMS) 122 que ejecuta los métodos aquí descritos. La infraestructura de terceros 103 incluye, además, dispositivos de almacenamiento 120 para almacenar datos históricos y actuales e relación con múltiples dispositivos bajo control remoto, además de información personal y financiera del cliente.

La infraestructura de terceros 103 puede ser cualquier sistema basado en Internet con el cual el usuario o cliente 113 establezca una relación con el fin de entablar el control del electrodoméstico 104 a través de comunicación inalámbrica desde la infraestructura de terceros 103 hacia el dispositivo 106, y desde el dispositivo 106 hacia el AMS 101. Los servidores 122 y los dispositivos de almacenamiento de datos 120 se muestran como entidades únicas en una ubicación discreta. En realidad, los servidores 122 y los dispositivos de almacenamiento 120 representan múltiples servidores y dispositivos de almacenamiento que pueden distribuirse en una red de cualquier modo. Los servidores 122 incluyen múltiples procesadores que ejecutan los métodos aquí descritos. En esta información, la infraestructura de terceros se describe como una infraestructura de pago, y el control del electrodoméstico se basa en el estado de la cuenta de pago del cliente 113 (que se transmite desde la infraestructura de terceros 103 al dispositivo para usuarios 106, y luego al AMS 101). No obstante, la base de la relación entre el usuario o cliente 113 y la infraestructura de tercero, y los eventos o motivos que controlan el electrodoméstico podrían no estar relacionados con los pagos. Por ejemplo, el sistema también pueden usarlo padres para controla diferentes electrodomésticos que usan sus hijos. Pero, a fines ilustrativos, a la infraestructura de terceros 103 aquí se hará referencia como una infraestructura de pagos.

En un diseño, la infraestructura de terceros 103 es un servicio de software que se ejecuta en servidores informáticos. Hace un seguimiento de cuando se realiza un pago para un electrodoméstico en particular, además de controlar el electrodoméstico. La infraestructura de pagos 103 se comunica con un proveedor de pagos 112 que pagos en efectivo o electrónicos 115 de parte de los clientes 113. Por ejemplo, el promovedor de pagos podría

ser PayPal, una empresa que gestiona pagos electrónicos; o podría ser un servicio de dinero móvil, como M-Pesa; o un banco, o Western Union, que les permite a los clientes depositar efectivo en tiendas minoristas y que ese dinero se acredite en una cuenta electrónica. El aspecto del pago no se considera un aspecto novedoso ni limitante de los diseños. En cambio, el evento del pago ocasiona que el sistema ejecute el método de control remoto, incluida la activación o desactivación del electrodoméstico 104.

La **Figura 2** es un diagrama de bloques de un diseño en la cual el dispositivo 106 también es el electrodoméstico 104. Por ejemplo, el dispositivo 106 puede ser un teléfono móvil que se controla de forma remota mediante la aplicación del software 102 de forma similar que lo que se describe en relación con la Figura 1. No obstante, el software/hardware/firmware del dispositivo 106/104 en sí mismo se usa para activar o desactivar el dispositivo 106/104. Fundamentalmente, el AMS es un software que se agrega al sistema operativo del dispositivo 106 (o al sistema operativo en sí mismo). Nuevamente, cuando el usuario 113 realiza pagos 115, y la infraestructura de pagos 103 los acepta, esta 103 entrega le entrega un comprobante de pago digital 109 con una firma digital 110 a la aplicación del software 102, la cual lo verifica, y controla el dispositivo 106/104 según corresponda.

La **Figura 3** es un diagrama de flujo en el que se ilustra un método 300 para el control remoto de electrodomésticos de acuerdo con un diseño como la de la Figura 1. En 302, un usuario o cliente le compra un electrodoméstico a un proveedor. En 304, el cliente descarga la aplicación de software de control del electrodoméstico (102) en su dispositivo (106). En 306, el cliente usa la aplicación del software para registrar una cuenta en línea con una infraestructura de pago (103). En 308, el subsistema de AMS transmite una ID e información de la cuenta al usuario del servicio 106 (a través de un cable USB en un diseño), y el dispositivo transmite la información a la infraestructura de pagos.

En 310, la aplicación del software determina si el período predeterminado ha expirado sin que el cliente presentara otros pagos (luego de un pago inicial al adquirir el electrodoméstico). Por ejemplo, el período puede ser un mes. Si el período no ha expirado,

el proceso continúa para verificar el vencimiento del período. Si este ha expirado sin otros pagos, el AMS desactiva el electrodoméstico en 312. La desactivación significa que el electrodoméstico no puede usarse, o que ciertas funciones predeterminadas de este no se pueden usar. La desactivación significa cortar la corriente o inhabilitar ciertas funciones.

En 314, cuando se envíe el pago a la infraestructura de pagos, esta creará un comprobante digital que incluirá información de la ID y una firma digital. La aplicación del software recibe un comprobante digital de forma inalámbrica en 316. En 318, se entrega un comprobante digital al AMS mediante un cable USB. Como se describió anteriormente, no es necesario el uso de un cable USB para llevar a la práctica la novedosa invención. Existen otros métodos dentro del alcance de la invención para comunicarse con otros elementos del sistema. En 320, el AMS intenta verificar el comprobante digital y determina (en 322) si la verificación se realizó correctamente. Si no fue así, se determina la naturaleza del error, y se envía un mensaje de error a la aplicación del software en 324.

Si la verificación del comprobante digital se realizó correctamente, el AMS activa el electrodoméstico en 326. La activación significa volver a habilitar cualquier característica o función que se hubiera inhabilitado en 312. Entonces, el proceso vuelve a 310 para esperar el vencimiento del próximo período.

En otros diseños, el período puede establecerse como menos o más de un mes. En otros diseños, el dispositivo 106 puede comunicarse con el AMS mediante Bluetooth, Wi-Fi, marcación por tonos (DTMF), modulación de la luz, código de barras 2D o 3D. El AMS 101 podría incluir un hardware estándar según su construcción original en el electrodoméstico, pero con firmware personalizado (software que se ejecuta en un microprocesador integrado).

Los diseños incluyen, además, diferentes interfaces de usuario que se presentan al usuario mediante un teléfono móvil, o cualquier otro dispositivo conectado a Internet. La interfaz de usuario puede brindar información completa en relación con la cuenta del cliente, como cuánto tiempo queda para que se inhabilite el electrodoméstico. Además, cualquier

información acerca de la cuenta financiera del cliente está disponible para este, lo cual incluye una descripción general de múltiples dispositivos que se financiaron de acuerdo con los diseños descritos, y un punto único en línea a través del cual los clientes pueden gestionar sus cuentas y controlar sus dispositivos (p. ej., prenderlos y apagarlos).

Las Figuras 4 a 8 son un sistema en diagramas de bloques en el cual se ilustran las configuraciones del sistema de control de electrodomésticos. En los diseños de las Figuras 4 a 8, el electrodoméstico que se controla es un teléfono móvil que también incluye un software controlador (como la aplicación 102). También se muestran métodos para prevenir que se manipule el software controlador. En primer lugar, la **Figura 4**, un sistema de control de electrodomésticos 400 incluye dispositivos 406A y 406B, que son teléfonos móviles que se pueden configurar de distintas formas, como se describe a continuación. Un gestor de arranque (o programa de gestión de arranque) es un componente del software de un dispositivo informático que se ejecuta al comienzo del proceso de encendido. Un ejemplo es un BIOS (sistema operativo integrado) en una computadora. Los teléfonos móviles tienen sistemas análogos. En los diseños, la aplicación del software 102 es parte de un sistema operativo (SO) 416 que hace funcionar un dispositivo 406. El SO 416 se instala en el dispositivo 406 mediante el mecanismo de "actualización" del gestor de cargas (a través del modo 408 de la interfaz del usuario de este), que les permite a los usuarios personalizar su SO o instalar uno nuevo. Como parte de la instalación del SO 416, el gestor de cargas está "bloqueado" para evitar cualquier otra actualización, que podría usarse para desinstalar el SO 416.

Como se describe en detalle a continuación, entre los diferentes métodos para bloquear el gestor de cargas se incluyen:

- alterar el código binario del programa del gestor de cargas para evitar que este reciba o valide nuevos paquetes de software;

- alterar los archivos del sistema operativo para que el gestor de cargas no pueda reconocerlos, mientras se mantiene la funcionalidad para el usuario;

- alterar los controladores del sistema de almacenamiento para que el gestor de cargas no pueda escribir nuevos archivos de datos;

modificar las direcciones de memoria para el sistema de almacenamiento del chip de memoria incorporado en el dispositivo para que las operaciones de escritura del gestor de cargas no tengan efecto en el dispositivo real; y

cuando un programa del gestor de cargas respalda un comando de "bloqueo", que emplea el bloqueo integrado, y, además, inhabilita el comando "desbloquear" del gestor de cargas al alterar el método de llamado de la función del software del comando "bloquear" para que no pueda funcionar cuando se lo llame con el método original; o alterar las claves criptográficas, o agregar nuevas, que se requieran para el comando "bloquear".

También en relación con la Figura 4, los dispositivos 406A y 406B son teléfonos móviles que se muestran intentado ingresar a un modo de interfaz de usuario del gestor de cargas 408 mediante distintos métodos.

El modo de la interfaz de usuario del gestor de cargas 408 es un modo en el cual un sistema operativo u otro software de sistema puede instalarse en un dispositivo. El software del sistema operativo, u otro sistema de software, también puede alterarse en este modo.

El teléfono móvil 406A muestra un patrón o una combinación de clave (o botón) de hardware que, al presionarse en simultáneo, permite al usuario acceder al modo de interfaz de usuario del gestor de cargas 408. El teléfono móvil 406B muestra un método alternativo de acceder al modo de interfaz de usuario del gestor de cargas 408. Como se muestra en 406B, hay un cable USB adjunto al dispositivo 406B y conectado a una computadora que permite la carga de archivos al dispositivo 406B, y la alteración de las configuraciones del dispositivo 406B y del firmware.

Se puede acceder a diferentes componentes de software y hardware 409 del dispositivo en este 406 cuando este 406 ingresa al modo de interfaz de usuario del gestor de cargas 408. Entre los componentes 409 se incluyen controladores de hardware 412, y un disco del dispositivo 414 con un esquema de direccionamiento asociado 415. Además, los componentes 409 incluyen un sistema operativo (SO), y una clave criptográfica que se usa para controlar el acceso al SO. Una clave criptográfica 411 está ubicada en el firmware 411 del dispositivo 406. Otra clave criptográfica 411 está integrada en el archivo del SO de

terceros 416. Estas claves deben coincidir antes de que el SO pueda instalarse en un dispositivo 406.

En un diseño, un SO de terceros 416 se carga en el dispositivo 406 mediante el modo de interfaz de usuario del gestor de cargas 408. En un diseño, el SO de terceros 416 incluye al menos una de las funcionalidades ejecutables de la aplicación de software 102 como se las describió anteriormente. En diferentes diseños, la alteración del SO 416 o de su funcionalidad se evita mediante diferentes métodos.

Como se muestra en la Figura 4, el acceso al modo de interfaz de usuario del gestor de cargas 408 está inhabilitado. En un diseño, el código binario del programa del gestor de cargas se altera para evitar que este reciba o valide nuevos paquetes de software.

La **Figura 5** es un diagrama de bloqueo de un sistema 500 en el que se ilustra una situación en la cual el electrodoméstico que se controla es un teléfono móvil que también incluye un software/hardware controlador. Los dispositivos 406A y 406B son teléfonos móviles que se muestran ingresando a un modo de interfaz de usuario del gestor de cargas 408 mediante distintos métodos.

El modo de la interfaz de usuario del gestor de cargas 408 es un modo en el cual un sistema operativo u otro software de sistema puede instalarse en un dispositivo. El software del sistema operativo, u otro sistema de software, también puede alterarse en este modo.

El teléfono móvil 406A muestra un patrón o una combinación de clave (o botón) de hardware que, al presionarse en simultáneo, permite al usuario acceder al modo de interfaz de usuario del gestor de cargas 408. El teléfono móvil 406B muestra un método alternativo de acceder al modo de interfaz de usuario del gestor de cargas 408. Como se muestra en 406B, hay un cable USB adjunto al dispositivo 406B y conectado a una computadora que permite la carga de archivos al dispositivo 406B, y la alteración de las configuraciones del dispositivo 406B y del firmware.

Se puede acceder a diferentes componentes de software y hardware 409 del dispositivo 406 cuando este 406 ingresa al modo de interfaz de usuario del gestor de cargas 408. Entre los componentes 409 se incluyen controladores de hardware 412, y un disco del dispositivo 414 con un esquema de direccionamiento asociado 415. Además, los componentes 409 incluyen un sistema operativo (SO), y una clave criptográfica que se usa para controlar el acceso al SO. En un diseño, un SO de terceros 416 se carga en el dispositivo 406 mediante el modo de interfaz de usuario del gestor de cargas 408. En un diseño, el SO de terceros 416 incluye al menos una de las funcionalidades ejecutables de la aplicación de software 102 como se las describió anteriormente. En diferentes diseños, la alteración del SO 416 o de su funcionalidad se evita mediante diferentes métodos. Como se muestra en la Figura 5, al modo de interfaz de usuario del gestor de cargas 408 se accede mediante métodos a los que se hace referencia en relación con los dispositivos 406A y 406B.

Cuando el software del gestor de cargas es compatible con un comando de "bloqueo", una clave criptográfica 410 se ubica en el firmware del dispositivo 406. Otra clave criptográfica 418 está integrada un archivo del SO. A fin de evitar el acceso no deseado a un SO de terceros 416, la clave criptográfica se cambia por una nueva y no publicada 410. Una persona que desee descargar un archivo del SO alterado en un dispositivo 406, no podrá hacerlo porque la nueva clave criptográfica del SO 418 no coincidirá con la clave criptográfica 410 del dispositivo no publicada.

En otros diseños en la que el software del gestor de cargas es compatible con el comando "bloquear", el bloqueo integrado está activado, y, además, el comando "desbloqueo" del gestor de cargas se inhabilita al evitar que el programa del gestor de cargas ejecute una llamada de comando "desbloqueo". En un diseño, esto se logra al alterar el método de llamado a la función del software del comando "desbloqueo" para que no pueda ejecutarse cuando se la llame con el método original de programa de gestor de cargas.

La **Figura 6** es un diagrama de bloques 600 en el que se ilustra otro método para evitar que se altere el SO del dispositivo o las funciones de este en un sistema similar al de las Figuras 4, 5 y 7-8. Cuando un gestor de cargas recibe un nuevo archivo de SO, determina cómo

integrarlo en el SO existente. Esta integración podría suceder mediante la sobreescritura de ciertos archivos o ciertas carpetas 417 en el disco del dispositivo 414. Para prevenir esta sobreescritura, el SO de terceros 416 reconfigura los nombres de archivos y carpetas de archivos para que no coincidan con los que pretende sobreescribir un SO "nuevo" no deseado. La funcionalidad del dispositivo se mantiene en todos los otros aspectos. Por ejemplo, como se muestra en 417, la carpeta "sistema" puede cambiarse por "pruebas".

La **Figura 7** es un diagrama de bloques 700 en el que se ilustra otro método para evitar que se altere el SO del dispositivo o las funciones de este en un sistema similar al de las Figuras 4-6 y 8. Cuando un gestor de cargas recibe un nuevo archivo de SO, determina cómo integrarlo en el SO existente. Esta integración podría suceder mediante la sobreescritura de ciertos archivos o ciertas carpetas en ciertas direcciones (físicas) de un disco sin formato en particular 415 en el disco del dispositivo 414. Para evitar esta sobreescritura, el SO de terceros 416 vuelve a numerar las direcciones de los discos sin formato para que no coincidan con las ubicaciones de sobreescritura designadas por un SO "nuevo" no deseado. La funcionalidad del dispositivo se mantiene en todos los otros aspectos.

La **Figura 8** es un diagrama de bloques 800 en el que se ilustra otro método para evitar que se altere el SO del dispositivo o las funciones de este en un sistema similar al de las Figuras 4-7. un diseño contempla una situación en la cual un usuario de dispositivos busca obtener acceso de lectura/escritura al disco del dispositivo 414 (p. ej., para sobreescribir el SO 416) al alterar los controladores del hardware del dispositivo 412. Para evitar esto, los controladores del hardware del dispositivo 412 se modifican a fin de no permitir el control de los diversos componentes de hardware del dispositivo mediante el modo de interfaz de usuario del gestor de cargas 408. De esta forma, el usuario que desea sobreescribir el SO 416 no es capaz de obtener acceso de lectura/escritura al disco del dispositivo 414.

En otros diseños, el sistema de control remoto del dispositivo aquí descrito habilita los modos de financiación. En una de estas formas, los clientes obtienen créditos al presentar un teléfono inteligente como garantía para:

(a) Financiación para un teléfono inteligente; o

(b) En general, cualquier intercambio que requiera una garantía. Por ejemplo, este puede ser el caso de un formulario de préstamos en el que la opción de controlar el dispositivo es garantía suficiente para el proveedor de la financiación.

Un teléfono inteligente puede volverse una garantía a demanda, es decir, en cualquier momento que el usuario (cliente, comerciante, otra entidad que tenga control del teléfono) desee que el teléfono se vuelva una garantía. Como resultado, esto permite un nuevo modelo comercial basado en la tecnología para los préstamos. En especial, un usuario es capaz de ofrecer control del software de su teléfono inteligente actual como garantía. A diferencia de los préstamos tradicionales, en lo que se requiere algún tipo de garantía monetaria o física, se puede ofrecer un teléfono inteligente como garantía sin tener que cederlo realmente o sin perder la capacidad de usarlo. Una vez que el préstamo se haya pagado en su totalidad, el software no ejercerá más un control sobre el dispositivo.

De hecho, permite que los prestamistas lleguen a nuevos grupos de usuarios. Los prestamistas pueden tomar más riesgos al ofrecerles un capital a los usuarios, quienes de otra forma no cumplirían los requisitos para el crédito (porque los usuarios no suelen tener otras garantías de alto valor para ofrecer). Como resultado, una gran cantidad de usuario podría acceder a créditos para los cuales lo cumplirían los requisitos habitualmente (porque no podrían ofrecer otras formas de garantías aceptadas).

Como ejemplo, el usuario final ("usuario") suele comenzar la operación para ofrecer el dispositivo como garantía. El consentimiento del usuario para ofrecer el dispositivo activa la ejecución de diferentes componentes de software a fin de "controlar el dispositivo". El usuario podría acceder a la interfaz del usuario de la aplicación del teléfono móvil 907 para iniciar el proceso de una de dos formas. El usuario puede hacer lo siguiente:

1. Descargar la aplicación de seguridad desde una tienda de aplicaciones pública como Google Play Store o directamente desde otro sitio web como payjoy.com. Luego, el usuario

acepta ofrecer el teléfono como garantía, y la aplicación de seguridad actualiza el Bloque de datos de control para marcar el teléfono como asegurado.

2. Además, en la iniciación del dispositivo, una aplicación privilegiada consulta a un servidor, y si este especifica que el dispositivo debería controlarse, entonces la aplicación privilegiada instalará automáticamente la aplicación de seguridad.

La **Figura 9** es un diagrama de bloques en el que se ilustra un diseño que permite la financiación para usuarios de teléfonos móviles. El teléfono inteligente 900 es el teléfono móvil del usuario. El teléfono inteligente 900 aloja la aplicación privilegiada 901, el bloque de datos de control 903 y la aplicación de seguridad 906.

La aplicación privilegiada 901 abarca la ejecución de un proceso mediante el cual se brindan privilegios de sistema operativo especiales para instalar la aplicación de seguridad (906) con los privilegios requeridos para controlar el dispositivo.

La verificación de la firma 902 la realiza la aplicación privilegiada 901 a fin de verificar si el dispositivo debe controlarse. La verificación de la firma 902 determina que la aplicación privilegiada 901 está autorizada para modificar el bloque de datos de control 903. Esta verificación es necesario porque el bloque de datos de control 903 es un área sensible del sistema. Únicamente el software del teléfono inteligente (y otras aplicaciones autorizadas, habitualmente aplicaciones del sistema con firma de la plataforma) debería poder acceder el bloque de datos de control.

El bloque de datos de control 903 es una serie de bytes reservados en un área de datos protegida que no puede restablecerse (no se borra durante la "restauración de fábrica") que se usa para garantizar el uso correcto de dispositivos que pueden controlarse mediante el software del dispositivo. La aplicación privilegiada (901) inspeccionará estos datos para detectar si el dispositivo debe ser controlado por el software. Si el dispositivo cumple con los requisitos para la financiación, la aplicación privilegiada (901) se pondrá en contacto con el servidor (904) para descargar la aplicación de seguridad (906). Únicamente el software (y otras aplicaciones del sistema con permisos especiales) tiene acceso al bloque

de datos de control 903. El servidor 904 es análogo al procesador 122 de la Figura 1 que lo opera otro proveedor del método y sistema de financiación aquí descrito.

El servidor 904 es confiable para la aplicación privilegiada (901), que contacta al servidor 904 para iniciar el control del dispositivo. El servidor 904 descarga la aplicación de seguridad (906), que se instala en la aplicación privilegiada (901) en la ubicación correcta del dispositivo. La aplicación de seguridad 906 controla el dispositivo al bloquearlo y desbloquearlo.

La comunicación del servidor 905 es una comunicación segura entre la aplicación privilegiada (901) y el servidor (904) para iniciar la descarga de la aplicación de seguridad (906) y para intercambiar información relacionada y de la configuración del dispositivo.

La aplicación de seguridad 906 bloquea y desbloquea el dispositivo en función de la información que obtiene del servidor 904 (o del software del dispositivo) acerca del rendimiento de pagos del usuario.

Las **Figuras 10 a 16** son capturas de pantalla en las que se ilustra una aplicación de bloqueo de teléfono en función de los diseños. La aplicación de bloqueo de teléfono es un elemento de la aplicación de seguridad, que se le representa al cliente/usuario a través de una interfaz de usuario provista, en este caso, por PayJoy, y que se ilustra en las Figuras. La "Aplicación PayJoy" hace referencia, en general, a la aplicación del usuario en el teléfono que realiza las funciones aquí descritas, y presenta la interfaz de usuario aquí descrita.

La **Figura 10** es una captura de pantalla en la que se muestra que el usuario tiene 6 horas de crédito restante en el teléfono. También se muestra la fecha límite de pago. En la parte inferior, se muestran los botones que le permiten al usuario pagar, solicitar ayuda o navegar al inicio de la aplicación PayJoy. Los botones inactivos aparecen en gris.

La **Figura 11** es una captura de pantalla en la que se muestra que el usuario tiene 6 horas de crédito restante en el teléfono. También se muestra la fecha límite de pago, y que no se detecta una tarjeta SIM en el teléfono. El usuario no puede realizar una llamada, pero puede

navegar a "configuraciones". En la parte inferior, se muestran los botones que le permiten al usuario pagar, solicitar ayuda o navegar al inicio de la aplicación PayJoy. Los botones inactivos aparecen en gris.

La **Figura 12** es una captura de pantalla en la que se muestra que al usuario se le solicita realizar un pago en la tienda de PayJoy más cercana. En la pantalla también se informa que el teléfono debe estar conectado a Internet luego de que se haya realizado el pago para garantizar que se actualice el crédito del usuario. Si el usuario no tiene acceso a Internet, se le recomienda comunicarse con el soporte para obtener un código y actualizar su crédito. En la parte inferior, se muestran los botones que le permiten al usuario pagar, solicitar ayuda o navegar al inicio de la aplicación PayJoy. Los botones inactivos aparecen en gris.

La **Figura 13** es una captura de pantalla en la que se muestran opciones que tiene el usuario para realizar una llamada de emergencia, llamar a Atención al cliente o ir a configuraciones del teléfono. En la parte inferior, se muestran los botones que le permiten al usuario pagar, solicitar ayuda o navegar al inicio de la aplicación PayJoy. Los botones inactivos aparecen en gris.

La **Figura 14** es una captura de pantalla en la que se muestra que se notifica al usuario que no hay conexión a Internet. Se recomienda al usuario verificar las configuraciones del Wi-Fi y los datos del plan de la compañía telefónica. Además, el usuario puede hacer clic para ingresar el código recibido anteriormente. Al usuario se le indica que tiene 6 horas de crédito restante, y que la fecha límite para el próximo pago es el 21 de octubre de 2020. En la parte inferior, se muestran los botones que le permiten al usuario pagar, solicitar ayuda o navegar al inicio de la aplicación PayJoy. Los botones inactivos aparecen en gris.

La **Figura 15** es una captura de pantalla en la que se muestra que el usuario no tiene más crédito. También se le notifica que no se detecta ninguna tarjeta SIM. Se muestra la fecha de pago para el siguiente pago. En la parte inferior, se muestran los botones que le permiten al usuario pagar, solicitar ayuda o navegar al inicio de la aplicación PayJoy. Los botones inactivos aparecen en gris.

La **Figura 16** es una captura de pantalla en la que se muestra que se notifica al usuario que no hay conexión a Internet. Se recomienda al usuario verificar las configuraciones del Wi-Fi y los datos del plan de la compañía telefónica. Además, el usuario puede hacer clic para ingresar el código recibido anteriormente. Se le notifica que no se detecta ninguna tarjeta SIM. Al usuario se le indica que no tiene crédito restante y que la fecha límite para el próximo pago es el 21 de octubre de 2020. En la parte inferior, se muestran los botones que le permiten al usuario pagar, solicitar ayuda o navegar al inicio de la aplicación PayJoy. Los botones inactivos aparecen en gris.

Mediante la estructura presente en las Figuras 1 a 9, se habilitan otros diseños, como se describe a continuación. Estos otros diseños se le presentan al usuario a través de pantallas de interfaz de usuario similares a las de las Figuras 10 a 16, según corresponda, y pueden llevarse a la práctica mediante una aplicación de pago que funciona por encima o a través de la aplicación de bloqueo.

En función del diseño, el teléfono puede desbloquearse mediante un código, incluso si debiera estar bloqueado por contrato. El cliente (usuario) tiene permitido un período de gracia durante el cual puede seguir usando el teléfono, aunque no haya realizado un pago. Por ejemplo, si el cliente no realizó el pago y se ha bloqueado el teléfono, puede comunicarse con el Acreedor (p. ej., Atención al cliente cuya información de contacto se encuentra en la Aplicación PayJoy. El cliente puede seguir usando la Aplicación PayJoy, aunque el teléfono haya sido bloqueado) para obtener un "Código de desbloqueo" especial. El cliente ingresa este código en la Aplicación PayJoy, y esta autentica la validez del código y desbloquea el teléfono durante un período específico.

En otro diseño, el cliente recibe una función de "Línea vital". Al presionar el botón correcto en la interfaz de usuario, la aplicación PayJoy le otorga automáticamente al cliente un período fijo por el cual el teléfono permanecerá desbloqueado, aunque no haya realizado un pago. Esto es útil si el cliente se encuentra en una emergencia (p. ej., desastre natural,

problemas de seguridad personal, etc.) y no pueden realizar un llamado para obtener un código (como en el diseño anterior), pero requiere acceso al teléfono por un período.

Otro diseño es, en esencia, un bloqueo de red que bloquea el teléfono frente a una red de comunicaciones determinada (p. ej., una red de compañía telefónica o punto de acceso a Wi-Fi). Además de bloquear el teléfono cuando el usuario no realiza un pago, siempre impone una regla de que el teléfono solo debe usarse para una red de comunicaciones determinada. Esto puede permitir que las compañías telefónicas y otros terceros hagan que la financiación de dispositivos funcione en conjunto con otros modelos comerciales. Por ejemplo, esto podría permitirles a las compañías telefónicas reducir aún más el precio de la financiación, dado que tienen la garantía de que el cliente solamente usará el teléfono otorgado en su red.

En otro diseño, los clientes reciben un período agregado antes de su próximo pago a cambio de recomendaciones. Por ejemplo, si un cliente le recomienda PayJoy a 10 clientes, recibe 10 días de crédito antes de la próxima fecha de pago.

En otro diseño, los clientes podrían realizar pagos por otros amigos o familiares. Por ejemplo, en el caso de que un cliente sea el cosignatario de su cónyuge. En este caso, el cliente puede realizar pagos desde su teléfono por el teléfono de su cónyuge. Estarían sujetos a los términos de la financiación de dispositivos. Es decir, pueden elegir si, en caso de no realizar un pago, se bloquea el teléfono del cliente, o del cónyuge. La opción de qué teléfono se bloquea también puede controlarla el acreedor que financia el teléfono.

En otro diseño, el teléfono se bloquea parcialmente por falta de pago. Cuando el cliente no realiza un pago, en vez de bloquear todo el teléfono, se inhabilitan ciertas funciones del teléfono. Por ejemplo, se puede inhabilitar el acceso a aplicaciones de mensajería como WhatsApp, o a aplicaciones de SMS o video, como TikTok. Al mismo tiempo, pueden permitirse las llamadas entrantes y salientes.

En otro diseño, los clientes/usuarios cumplen los requisitos para devoluciones de efectivo en una billetera móvil luego de pagar su préstamo.

En otro diseño, una vez que se haya demostrado que el usuario es confiable, se le concede una línea de crédito.

Los aspectos del sistema y los métodos aquí descritos pueden ponerse en uso como una funcionalidad programada en cualquiera de diferentes circuitos, incluidos los dispositivos lógicos programables (PLD), como las matrices de puertas lógicas programable in situ (FPGA), los dispositivos de matriz de lógica programable (PAL), los dispositivos de memoria y lógica programable eléctricamente y los dispositivos estándares basados en la celdas, además de circuitos integrados para aplicaciones específicas (ASIC). Otras posibilidades para poner en práctica aspectos del sistema incluyen: microcontroladores con memoria (memoria de solo lectura eléctricamente programable y borrrable (EEPROM)), microprocesadores incorporados, firmware, software, etc. Asimismo, ciertos aspectos del sistema pueden integrarse en microprocesadores con emulación de circuitos basados en software, lógica discreta (secuencial y combinatoria), dispositivos personalizados, lógica difusa (neural), dispositivos cuánticos, e híbridos de cualquier de estos tipos de dispositivos. Por supuesto, las tecnologías de dispositivos subyacentes pueden brindarse mediante diferentes tipos de componentes, p. ej., tecnologías de transistor de efecto de campo de semiconductor de óxido metálico (MOSFET) como semiconductor de complementario de óxido metálico (CMOS), tecnologías bipolares como lógica de emisores acoplados (ECL), tecnologías de polímeros (p. ej., polímero de silicón conjugado y estructuras de metal-polímero conjugadas con metal), mezcla de análogo y digital, etc.

Debe tenerse en cuenta que las diferentes funciones y los distintos procesos detallados aquí pueden describirse como datos o instrucciones incluidas en diferentes medios legibles por computadoras, en términos de su transferencia de registro y conducta, componente lógico,

transistor, geometría del diseño, u otras características. Entre los medios legibles por computadoras en los cuales dichos datos o instrucciones formateados pueden incorporarse se incluyen, entre otros, medio de almacenamiento no volátil en diversas formas (p. ej., medio de almacenamiento de semiconductor, magnético u óptico) y ondas portadoras que podrían usarse para transferir dichos datos o instrucciones formateadas mediante medios de señales por cable, ópticos o inalámbricos, o cualquier combinación de estos. Entre los ejemplos de transferencias de dichos datos o instrucciones formateados por parte de ondas portadoras se incluyen, entre otros, transferencias (cargas, descargas, correo electrónico, etc.) mediante Internet u otras redes informáticas por uno o más protocolos de transferencia de datos (p. ej., HTTP, FTP, SMTP, etc.). Cuando se los reciba dentro de un sistema informático mediante uno o más medios legibles por computadoras, las expresiones de componentes o procesos basadas en dichas instrucciones o datos dentro del sistema descrito podrían procesarse mediante una entidad de procesamiento (p. ej., uno o más procesadores) dentro del sistema informático en conjunto con la puesta en práctica de uno o más programas informáticos.

A menos que el contexto requiera lo contrario, a lo largo de la descripción y las reivindicaciones, las palabras "abarca", "abarcar" y términos similares deben comprenderse con un sentido inclusivo, en oposición a un sentido excluyente o exhaustivo; es decir, en el sentido de "incluye, entre otros...". Las palabras en singular o plural también incluyen su plural o singular respectivo. Asimismo, las palabras "aquí", "en lo sucesivo", "antes", "a continuación", y palabras similares hacen referencia a esta solicitud en su totalidad y no a partes específicas de esta. Cuando la palabra "o" se utiliza en relación con una lista de dos o más opciones, la palabra cubre las siguientes interpretaciones de la palabra: cualquiera de los elementos de la lista, todos los elementos de la lista, y cualquier combinación de los elementos de la lista.

La descripción previa de los diseños ilustrados de los sistemas y los métodos no pretende ser exhaustiva ni limitar los sistemas y métodos a las formas precisas detalladas- Si bien los diseños específicos y los ejemplos de métodos y componentes de los sistemas se

describen aquí con fines ilustrativos, pueden realizarse diferentes modificaciones equivalentes dentro del alcance de los sistemas, componentes y métodos, como reconocerán quienes tengan conocimientos sobre los dibujos pertinentes. La información sobre los métodos y sistemas aquí brindada puede aplicarse a otros métodos y sistemas de procesamiento, no solo para los aquí descritos.

Los elementos y las acciones de los diferentes diseños antes descritos pueden combinarse para brindar incluso más diseños. Según la detallada descripción anterior, pueden realizarse estos y otros cambios a los métodos y sistemas.

En general, en las siguientes reivindicaciones, los términos usados no deben interpretarse como una limitación de los métodos y sistemas a los diseños específicos detallados en la especificación y en las reivindicaciones, sino que deben entenderse como que incluyen todos los sistemas de procesamiento que funcionan en relación con las reivindicaciones. Del mismo modo, los métodos y sistemas no se limitan en función de la información brindada, sino que el alcance de los métodos y sistemas debe determinarse completamente por las reivindicaciones.

Si bien ciertos aspectos de los métodos y sistemas se presentan a continuación en formas de reivindicación específicas, los inventores contemplan los diferentes aspectos de los métodos y sistemas en cualquier formulario de reivindicación. Por ejemplo, si bien solo un aspecto de los métodos y sistemas puede enumerarse como integrado en el medio legible por la máquina, otros aspectos pueden también estar integrados en el medio legible por la máquina. Del mismo modo, los inventores se reservan el derecho de agregar reivindicaciones adicionales luego de presentar la solicitud para completar formularios adicionales de reivindicación para otros aspectos de los métodos y sistemas.