(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 746 985**

(51) Int. CI.:

G06F 21/60 (2013.01)
G06F 21/74 (2013.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **22.04.2014 PCT/KR2014/003496**

(87) Fecha y número de publicación internacional: **30.10.2014 WO14175630**

(96) Fecha de presentación y número de la solicitud europea: **22.04.2014 E 14787929 (0)**

(97) Fecha y número de publicación de la concesión europea: **21.08.2019 EP 2989585**

(54) Título: **Aparato y procedimiento de notificación de información de seguridad en un dispositivo electrónico y medio de grabación legible por ordenador para el mismo**

(30) Prioridad:

24.04.2013 KR 20130045782

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
09.03.2020

(73) Titular/es:

SAMSUNG ELECTRONICS CO., LTD. (100.0%)
129, Samsung-roYeongtong-gu
Suwon-si, Gyeonggi-do, 443-742, KR

(72) Inventor/es:

HEO, YOUNKYU;
KIM, YOUNGKYOO;
KIM, MOOYOUNG;
KIM, MINJUNG;
JANG, DONGHO y
CHUN, JAEBONG

(74) Agente/Representante:

CARPINTERO LÓPEZ, Mario

DESCRIPCIÓN

Aparato y procedimiento de notificación de información de seguridad en un dispositivo electrónico y medio de grabación legible por ordenador para el mismo

Campo técnico

La presente invención se refiere por lo general a un aparato y un procedimiento para la notificación de información en un dispositivo electrónico, y más particularmente, a un aparato y un procedimiento para notificar información que requiere seguridad en un dispositivo electrónico.

Antecedentes de la técnica

El uso de terminales de comunicación inalámbrica, como dispositivos electrónicos, dispositivos móviles, teléfonos inteligentes, tabletas, ordenadores personales (PC) y similares, ha aumentado tanto en la vida personal del usuario como en el mundo de los negocios, y la utilización de los terminales comunicación inalámbrica para tareas dentro de las empresas ha aumentado también.

De acuerdo con el aumento en la utilización de los terminales de comunicación inalámbrica en las empresas, tales como las empresas y corporaciones, ha surgido un problema relacionado con la seguridad del terminal de comunicación inalámbrica para procesar documentos u otros datos utilizados en una empresa. En consecuencia, para mejorar la seguridad de los terminales de comunicación inalámbrica, las compañías de seguridad han desarrollado soluciones de seguridad que se pueden agregar a los terminales de comunicación inalámbrica, y estas soluciones de seguridad se venden en un mercado empresa a empresa (B2B).

El documento US 2010/0070980 A1 se refiere a un sistema de detección de eventos, un procedimiento de detección de eventos y un programa. El sistema informático de detección de eventos incluye: una pluralidad de máquinas virtuales para implementar entornos de ejecución virtual; una porción de detección de eventos para detectar un evento que ha ocurrido en los entornos de ejecución virtuales; y una porción de presentación de eventos para presentar, cuando un evento ocurrido en el entorno de ejecución virtual no mostrado en el dispositivo de visualización que está siendo detectado por la porción de detección de eventos, la información del evento relativa al evento ocurrido en el entorno de ejecución virtual en un entorno de ejecución virtual actualmente visualizado en el dispositivo de visualización.

El documento US 2008/0082936 A1 se refiere a un procedimiento y sistema para mostrar datos de tareas alternativas en un dispositivo electrónico móvil. El mismo desvela un dispositivo electrónico móvil y un procedimiento para el mismo que, de una forma mínimamente disruptiva, informa al usuario de datos de tareas alternativas y proporciona un mecanismo en pantalla para que el usuario seleccione tareas alternativas o regrese a la visualización no disruptiva de los datos de tareas actuales. Una vez que dicho procedimiento comprende la representación en una pantalla de un dispositivo electrónico móvil en una ventana de primer tamaño los datos de una primera tarea, detectar en el dispositivo un evento que involucra una segunda tarea y, en respuesta al evento, representar en la pantalla del dispositivo en una ventana de segundo tamaño los datos de la primera tarea mientras se muestra adyacente a la ventana de segundo tamaño un panel adaptado para informar al usuario del evento. El panel puede incluir información del evento y un menú adaptado para recibir una selección de usuario con respecto al evento.

El documento US 2005/0204138 A1 se refiere a un sistema y procedimiento para un protector de pantalla de correo electrónico. El mismo proporciona un sistema y un procedimiento para un protector de pantalla de correo electrónico. En un ejemplo, el procedimiento incluye la supervisión de actividad y, si no se detecta actividad dentro de un período de tiempo predefinido, la activación de un protector de pantalla. Si se recibe un mensaje, el procedimiento determina si el protector de pantalla está activo e identifica una configuración de notificación de mensaje si el protector de pantalla está activo, en el que la configuración de notificación de mensaje identifica al menos un destino definido por el usuario en el que se notificará a un usuario. El usuario recibe una notificación del mensaje recibido en el destino. A continuación se ejecuta una rutina de autorización para determinar si el usuario ha ingresado un código de autorización correcto, y el mensaje se le proporciona al usuario en el destino sin desactivar el protector de pantalla si el usuario ha ingresado el código de autorización correcto.

El documento US 7.689.939 B1 se refiere a la ruptura de una aplicación de software a través de un protector de pantalla. El mismo se refiere a un ordenador personal que incluye: un dispositivo de visualización para mostrar información de imagen y un procesador operable cuando el dispositivo de visualización está en el modo de protector de pantalla para (a) recibir, desde una aplicación, al menos parte de la que se está ejecutando en un ordenador personal, una notificación de la ocurrencia de un evento; (b) determinar si el evento es miembro de un conjunto definido de eventos; y (c) cuando el evento es miembro del conjunto definido de eventos, mostrar en la pantalla la información de imagen asociada con el evento, en el que la función de visualización ocurre mientras la pantalla está en el modo de protector de pantalla.

Divulgación de la invención

Problema técnico

Las soluciones de seguridad de dispositivos B2B representativas que se utilizan actualmente en los terminales de comunicación inalámbrica incluyen VMWare y un procedimiento de división del sistema operativo.

Cuando se usa VMWare, se ejecuta un procedimiento separado para usar aplicaciones de áreas de memoria divididas. El procedimiento para usar las aplicaciones de las áreas divididas ocupa una memoria para ejecutar el procedimiento correspondiente y el procedimiento correspondiente es ejecutado por una Unidad Central del tratamiento (CPU). En consecuencia, cuando se usa VMWare, se necesita una memoria adicional para ejecutar el procedimiento y también se necesita una CPU de alta velocidad.

Puesto que el procedimiento de división del SO ejecuta los SO respectivos al mismo tiempo o el cambio de la ejecución de los SO no es gratuito, no es fácil recibir, en tiempo real, información de diferentes áreas que le dan importancia a la transferencia en tiempo real, por ejemplo, una notificación por correo electrónico.

Es decir, las soluciones de seguridad de los terminales de comunicación inalámbrica que se han proporcionado hasta ahora tienen todavía dificultades para mostrar la información que se debe proteger mientras se asegura la transferencia en tiempo real.

Solución al problema

Ciertas realizaciones de la presente divulgación proporcionan un aparato y un procedimiento para mostrar información que debe protegerse en un dispositivo electrónico.

Ciertas realizaciones de la presente divulgación proporcionan un aparato y un procedimiento para mostrar, en tiempo real, la información que debe protegerse en un dispositivo electrónico.

Ciertas realizaciones de la presente divulgación proporcionan un aparato y un procedimiento para mostrar, en tiempo real, la información que se debe proteger y la información que no se requiere proteger en un dispositivo electrónico, y mostrar información que no se requiere proteger después de eliminar la información mostrada que debe estar protegida de la información a proteger.

De acuerdo con un aspecto de la presente invención, se proporciona un procedimiento para controlar la información usando un dispositivo electrónico, el procedimiento comprende: reconocer la generación de información de notificación de uno o más procedimientos activados en un primer modo de operación entre una pluralidad de modos de operación que incluyen el primer modo de operación y un segundo modo de operación; y notificar a un usuario de solo una parte de la información de notificación cuando un modo de operación actual es el segundo modo de operación, en el que la parte de la información de notificación proporciona menos información que la información de notificación, y la información de notificación incluye al menos un número de veces que la información de notificación se ha generado para el usuario.

De acuerdo con otro aspecto de la presente invención, se proporciona un dispositivo electrónico que comprende: un conjunto de módulos de reconocimiento para reconocer la generación de información de notificación de uno o más procedimientos activados en un primer modo de operación entre una pluralidad de modos de operación que incluyen el primer modo de operación y un segundo modo de operación; y un módulo de notificación configurado para notificar a un usuario solo una parte de la información de notificación cuando un modo de operación actual es el segundo modo de operación en el que la parte de la información de notificación proporciona menos información que la información de notificación, y la información de notificación incluye al menos un número de veces que la información de notificación se ha generado para el usuario.

De acuerdo con otro aspecto de la presente invención, se proporciona un medio de almacenamiento que almacena comandos, los comandos se configuran para permitir que uno o más procedimientos realicen una o más operaciones cuando los comandos son ejecutados por uno o más procedimientos, comprendiendo la una o más operaciones: reconocer la generación de información de notificación de uno o más procedimientos activados en un primer modo de operación entre una pluralidad de modos de operación que incluyen el primer modo de operación y un segundo modo de operación; y notificar a un usuario de solo una parte de la información de notificación cuando un modo de operación actual es el segundo modo de operación, en el que la parte de la información de notificación proporciona menos información que la información de notificación, y la información de notificación incluye al menos un número de veces que la información de notificación se ha generado para el usuario.

Efectos ventajosos de la invención

Para usar dispositivos electrónicos para un fin comercial, las compañías ofrecen por separado dispositivos electrónicos de oficina a sus empleados, o montan una solución de seguridad para dispositivos electrónicos personales para un fin individual propiedad de los empleadores (empleados) para usar el dispositivo electrónico personal en la compañía. Cuando un dispositivo electrónico utilizado con fines comerciales se utiliza para un fin individual en un caso particular, los requisitos entre el empleador y el empleado con frecuencia entran en conflicto entre sí.

Por ejemplo, existe un conflicto cuando el empleador requiere que se monte una solución de seguridad particular en el dispositivo electrónico para proteger de forma segura la propiedad de la compañía y el empleado desea proteger la información personal correspondiente a la privacidad de la compañía.

Para satisfacer las demandas tanto del empleador como del empleado, se admiten espacios separados para aplicaciones o datos para fines comerciales y aplicaciones o datos para fines individuales, y por lo tanto se puede proporcionar la seguridad del dispositivo electrónico.

Se puede establecer un modo de seguridad para cifrar datos y almacenar los datos cifrados en un área de memoria que está separada de un modo sin seguridad y asignado al modo de seguridad. El modo de seguridad se puede configurar para permitir que solo los usuarios autenticados accedan a los datos almacenados en el área de memoria asignada al modo de seguridad. El modo sin seguridad puede ser un conjunto de modos que no requiere cifrado o autenticación para acceder a los datos.

Por ejemplo, cuando se detecta una solicitud de acceso a los recursos configurados para ser accesibles solo en el modo de seguridad mientras está activado el modo sin seguridad, la solicitud de acceso detectada puede bloquearse primero y una solicitud de autenticación adicional para el acceso a los recursos en el modo de seguridad puede hacerse al usuario.

El usuario del dispositivo electrónico experimenta muchos inconvenientes en el modo de seguridad descrito anteriormente.

Por ejemplo, cuando se genera una notificación del uso para el fin individual, se producen sucesivamente situaciones en las que se viola la seguridad y el dispositivo electrónico informa al usuario de la violación de seguridad en la situación de violación de seguridad. En consecuencia, cuando el usuario del dispositivo electrónico usa el dispositivo electrónico en el modo de seguridad, las notificaciones de la violación de seguridad de acuerdo con la notificación del uso para el fin individual se emiten en exceso. Esto suele ser contrario a las políticas del empleador.

Por el contrario, cuando el usuario usa el dispositivo electrónico para un fin individual (en lo sucesivo denominado "modo sin seguridad"), se pueden generar notificaciones utilizadas para un correo electrónico de la compañía u otras áreas comerciales de la compañía. En este caso, los asuntos que se deben asegurar se proporcionan al usuario a través de la notificación en el modo sin seguridad, y la empresa puede experimentar fugas no deseadas de información.

Breve descripción de los dibujos

Los anteriores y otros aspectos, características y ventajas de la presente invención serán más evidentes a partir de la siguiente descripción detallada junto con los dibujos adjuntos, en los que:

la Figura 1 es un diagrama de bloques que ilustra un aparato electrónico de acuerdo con una realización de la presente divulgación;
la Figura 2 es una vista de procedimientos para controlar por separado las operaciones de un modo sin seguridad y un modo de seguridad en un dispositivo electrónico y mostrar las operaciones controladas por separado de acuerdo con una realización de la presente invención;
la Figura 3 ilustra un ejemplo de una pantalla que muestra un mensaje de notificación de un modo sin seguridad y un mensaje de notificación de un modo de seguridad en una unidad de visualización de un dispositivo electrónico de acuerdo con las realizaciones de la presente invención;
las Figuras 4A y 4B ilustran ejemplos de pantallas para describir casos en los que se requiere acceso a un modo configurado actualmente y otro modo y el acceso se rechaza de acuerdo con las realizaciones de la presente invención;
la Figura 5 es una vista que describe operaciones de procedimientos cuando un dispositivo electrónico que tiene un modo de seguridad y un modo sin seguridad descarga una aplicación en el modo de seguridad e instala la aplicación descargada en el modo de seguridad de acuerdo con las realizaciones de la presente invención;
la Figura 6 es una vista que describe un procedimiento de visualización cuando un dispositivo electrónico que tiene un modo sin seguridad y un modo de seguridad comparte una interfaz independientemente del modo de acuerdo con las realizaciones de la presente invención;
la Figura 7 es un diagrama de bloques de un dispositivo electrónico de acuerdo con diversas realizaciones de la presente divulgación; y
la Figura 8 es un diagrama de flujo de un procedimiento de notificación de información limitada de acuerdo con las realizaciones de la presente invención.

Mejor modo para llevar a cabo la invención

En lo sucesivo en el presente documento, se describirán las realizaciones de la presente invención con referencia a los dibujos adjuntos. Los dibujos adjuntos de esta memoria descriptiva se proporcionan para ayudar a comprender las realizaciones de la presente invención y debe observarse que la presente invención no está limitada por los tipos o diseños ilustrados en los dibujos adjuntos de esta memoria descriptiva. Además, los equivalentes o extensiones de las realizaciones adicionales de los dibujos adjuntos de esta memoria descriptiva deben entenderse por la descripción que hace referencia a los dibujos.

De acuerdo con las realizaciones desveladas en esta memoria descriptiva, cuando se requiere que se muestre información de notificación de un modo de seguridad mientras un dispositivo electrónico que tiene el modo de seguridad y un modo sin seguridad opera en el modo sin seguridad, una indicación que informa al usuario que existe

información de notificación en el modo de seguridad puede mostrarse en tiempo real. En consecuencia, el usuario puede detectar inmediatamente la generación de la información de notificación en el modo de seguridad para tomar medidas a tiempo.

Además, cuando se requiere que la información de notificación en el modo de seguridad se muestre en el modo sin seguridad, el dispositivo electrónico proporciona cierta información, como un tipo de evento que indica qué evento se ha generado y la cantidad de eventos generados, evitando así la filtración de información innecesaria.

Las realizaciones desveladas en esta memoria descriptiva proporcionan un procedimiento de visualización capaz de proporcionar seguridad cuando se genera un evento que se debe asegurar, como el correo electrónico de una empresa, en el dispositivo electrónico, que puede usarse tanto en el modo de seguridad como en el modo sin seguridad, y se muestra un mensaje de notificación del evento.

El dispositivo electrónico de acuerdo con diversas realizaciones de la presente invención puede ser un ordenador personal de escritorio (PC), un ordenador portátil, un asistente digital personal (PDA), un reproductor multimedia portátil (PMP), una tableta, un teléfono móvil, un vídeo teléfono, un teléfono con funciones, un teléfono inteligente, un lector de libros electrónicos, una cámara digital, un dispositivo portátil, un dispositivo inalámbrico, un sistema de Sistema de Posicionamiento Global (GPS), un dispositivo portátil, un reproductor de MP3, una videocámara, un juego consola, un reloj electrónico, un dispositivo de panel plano, una fotografía electrónica, una pizarra electrónica, un letrero electrónico, un proyector, un dispositivo de navegación, una caja negra, un decodificador, un diccionario electrónico, un refrigerador, un aire acondicionado, una aspiradora, un robot de inteligencia artificial, un Televisor (TV), un reproductor de disco versátil digital (DVD), un equipo de música, un horno, un horno de microondas, una lavadora, un filtro de aire, un dispositivo médico, un dispositivo de vehículo , un dispositivo de construcción naval, un dispositivo de aeronave, un dispositivo de seguridad, equipo agrícola, vacuno, de pesca, ropa electrónica, una llave electrónica, un brazalete electrónico, un collar electrónico y similares. Por ejemplo, los dispositivos electrónicos pueden estar controlados por varios sistemas operativos, como Android, iOS, Windows, Linux, Symbian, Tizen y Bada. Es evidente para los expertos en la materia que el dispositivo electrónico y el sistema operativo de acuerdo con las realizaciones de la presente invención no están limitados a los ejemplos descritos anteriormente.

La Figura 1 es un diagrama de bloques que ilustra el dispositivo electrónico de acuerdo con una realización de la presente invención.

El dispositivo electrónico incluye un módulo 110 de comunicación, una unidad 103 de cámara, una memoria 105, una unidad 106 de visualización, una unidad 107 de entrada y un controlador 111. El dispositivo electrónico puede incluir otros componentes, así como los componentes ilustrados en la Figura 1, o puede no incluir algunos de los componentes ilustrados en la Figura 1, por ejemplo, la unidad 103 de cámara.

El módulo 110 de comunicación incluye una antena ANT, una unidad 101 de radio, un módem 102, un micrófono MIC y un altavoz SPK. La antena ANT se fabrica de acuerdo con una banda para transmitir y recibir una señal de frecuencia requerida para la comunicación de un terminal portátil y se conecta a la unidad 101 de radio. En la siguiente descripción, se supone que el módulo 110 de comunicación accede a una red de comunicación móvil. Sin embargo, el módulo 110 de comunicación puede acceder a una red inalámbrica, tal como una Red de área local (LAN) inalámbrica, en lugar de la red de comunicación móvil. En este caso, todos los componentes ilustrados en la Figura 1 pueden incluirse también.

La unidad 101 de radio convierte sube de banda los datos que se transmitirán para la comunicación de voz y/o datos con la red de comunicación móvil y baja de banda los datos recibidos. Es decir, la unidad 101 de radio sube de banda los datos de una banda base para la transmisión de datos y transmite los datos a la red correspondiente a través de la antena ANT, y recibe una señal de radio de la red correspondiente a través de la antena ANT, baja de banda la señal de radio, y convierte la señal de radio en una señal de banda base.

El módem 102 realiza una serie del tratamiento de datos, tal como modulación, demodulación, codificación y decodificación de los datos. En la Figura 1, puesto que se supone que la comunicación de voz es posible, el módem 102 puede incluir un codificador de voz para realizar modulación/demodulación y codificación/decodificación de una señal de voz. Cuando se opera el codificador de voz, el módem 102 recibe una señal de voz eléctrica del micrófono MIC y convierte la señal de voz eléctrica recibida en una señal de voz digital, y codifica también la señal de voz digital. Además, cuando se opera el codificador de voz, el módem 102 convierte la señal de voz digital para que se envíe a una señal de voz eléctrica analógica y emite la señal de voz eléctrica analógica a través del altavoz SPK. En la comunicación de datos que no utiliza el codificador de voz, el módem 102 puede realizar una serie de operaciones, tales como modulación, demodulación, codificación y decodificación de datos para ser transmitidos/recibidos por un control del controlador 111.

La unidad 103 de cámara adquiere datos de imágenes fijas o datos de imágenes dinámicas recibiendo luz reflejada desde un asunto a través de una lente o convirtiendo la luz reflejada desde el asunto en una señal eléctrica. La unidad 103 de cámara convierte los datos de imagen fija adquiridos o los datos de imagen dinámica en datos que tienen el tipo que puede ser procesado por el controlador 111 y proporciona los datos convertidos al controlador 111.

La memoria 105 se refiere a un medio de almacenamiento, tal como una memoria de solo lectura (ROM) o una memoria

de acceso aleatorio (RAM) y almacena diversos datos de control necesarios para las operaciones del dispositivo electrónico. De acuerdo con las realizaciones de la presente invención, la memoria 105 almacena datos de control para operaciones de acuerdo con el modo de seguridad y el modo sin seguridad y datos para controlar una pantalla cuando se genera un evento particular en cada uno de los modos. Además, la memoria 105 puede incluir áreas para almacenar datos de usuario.

La unidad 106 de visualización puede implementarse en el tipo de un panel de pantalla de cristal líquido (LCD) o un panel de pantalla de emisión de luz (LED) y puede mostrar un estado del dispositivo electrónico en los procedimientos requeridos para las operaciones del dispositivo electrónico, y en un estado de espera, por un control del controlador 101. Además, la unidad 106 de visualización puede mostrar todos o algunos de los eventos generados de acuerdo con las realizaciones de la presente invención.

Además de la unidad 106 de visualización que transmite información visual, el dispositivo electrónico puede incluir además un componente adicional que puede transmitir diversos tipos de información, como un sonido y una vibración al usuario.

La unidad 107 de entrada incluye todas las interfaces de entrada de usuario tales como una entrada táctil o/y un lápiz electrónico o/y una entrada de tecla. La unidad 107 de entrada recibe información de entrada del usuario a través de cada una de las interfaces de entrada y proporciona la información al controlador 111.

La Figura 2 es un diagrama de bloques de procedimientos para controlar por separado las operaciones en el modo sin seguridad y en el modo de seguridad en el dispositivo electrónico y mostrar las operaciones controladas por separado de acuerdo con una realización de la presente invención.

Como se ilustra en la Figura 2, hay dos modos separados en gran medida, como el modo sin seguridad que se muestra en el lado izquierdo y el modo de seguridad que se muestra en el lado derecho. El modo sin seguridad corresponde a un caso en el que el dispositivo electrónico se utiliza para fines individuales, y el modo de seguridad corresponde a un caso en el que el dispositivo electrónico se utiliza para fines comerciales en una empresa, como se ha descrito anteriormente. En la Figura 2, los bloques ilustrados en cada uno de los modos pueden ser procedimientos o servicios para operaciones particulares, y en lo sucesivo se supone que los bloques son todos procedimientos para conveniencia de la descripción.

En la Figura 2, el modo sin seguridad y el modo de seguridad pueden seleccionarse mediante un procedimiento (no mostrado en la Figura 2) para seleccionar cada modo. En consecuencia, solo se proporciona un modo al usuario a través de la unidad 106 de visualización. Cuando el usuario desea cambiar el modo sin seguridad al modo de seguridad, el cambio en el modo sin seguridad al modo de seguridad se realiza mediante un procedimiento de autenticación preestablecido.

En la Figura 2, un procedimiento 220 de mensaje de notificación sobre el modo sin seguridad y el modo de seguridad corresponde a un procedimiento para recopilar información de eventos proporcionada por un procedimiento particular en el modo sin seguridad o el modo de seguridad y mostrar la información de eventos recopilada en la unidad 106 de visualización a través de un procedimiento predeterminado. El procedimiento 220 de mensaje de notificación puede incluir un procedimiento 221 proxy de notificación en el modo de seguridad para recopilar y proporcionar información de eventos proporcionada por cada uno de los procedimientos en el modo de seguridad. Cuando el procedimiento 220 de mensaje de notificación no incluye el procedimiento 221 de proxy de notificación en el modo de seguridad, el procedimiento 220 de mensaje de notificación puede realizar una operación del procedimiento 221 de proxy de notificación en el modo de seguridad.

El procedimiento 221 de proxy de notificación en el modo de seguridad recibe información de eventos generada por todas las aplicaciones (en lo sucesivo, procedimientos 212, 213,..., 214 de "aplicación" que operan en el modo de seguridad y recopilan la información de eventos recibida, y pueden controlar los eventos generados por los procedimientos 212, 213,..., 214 de aplicación para que se muestren como un mensaje o se muestren, respectivamente.

Cada uno de los procedimientos en el modo sin seguridad se describirá primero. El modo sin seguridad incluye procedimientos necesarios cuando el usuario usa por lo general el dispositivo electrónico como se ha descrito anteriormente. Un procedimiento 201 de la tienda de aplicaciones es un procedimiento para acceder generalmente a una tienda de aplicaciones en el dispositivo electrónico. De acuerdo con la presente invención, el procedimiento 201 de la tienda de aplicaciones puede realizar conjuntamente una operación para acceder generalmente a la tienda de aplicaciones y una operación para acceder a la tienda de aplicaciones en el modo de seguridad. Esto se describirá más detalladamente con referencia a los dibujos que se describen a continuación.

Un procedimiento 205 del agente de gestión es un procedimiento requerido cuando se descarga una aplicación que se utilizará en el modo de seguridad. El procedimiento 205 del agente de gestión se describirá con más detalle en los dibujos que se describen a continuación.

Un primer procedimiento 202 de aplicación, un segundo procedimiento 203 de aplicación y un procedimiento 204 de aplicación de orden n pueden ser procedimientos de aplicación generales. Por ejemplo, los procedimientos 202, 203,...,

204 pueden ser procedimientos de aplicación para realizar un servicio de correo, una gestión de programación y un mensaje de texto, respectivamente.

A continuación, se describirán los procedimientos en el modo de seguridad. El modo de seguridad corresponde a un modo para la empresa que requiere la seguridad. En consecuencia, los procedimientos 212, 213,..., 214 restantes, excepto un procedimiento 215 de gestión en el modo de seguridad y un procedimiento 211 de la tienda de aplicaciones en el modo de seguridad, tienen que tener una función adicional para la seguridad.

En la siguiente descripción, se supone que un primer procedimiento 213 de aplicación en el modo de seguridad es un procedimiento para procesar un servicio de correo.

En general, el primer procedimiento 213 de aplicación en el modo de seguridad realiza un cifrado para mejorar la seguridad de los datos recibidos mientras realiza una operación para el servicio de correo. En consecuencia, el primer procedimiento 213 de aplicación en el modo de seguridad que proporciona el servicio de correo incluye un módulo para el cifrado y un proxy para inducir que los datos del servicio de correo se procesen en un modo de seguridad mejorado. Es decir, un procedimiento puede agregar el módulo para el cifrado y el proxy para la inducción del procesamiento de cifrado a las operaciones básicas del procedimiento.

Además, el primer procedimiento 213 de aplicación en el modo de seguridad incluye un procedimiento de, cuando se crea una dirección para almacenar datos generados, almacenar los datos de manera diferente del procesamiento mediante un procedimiento general. Es decir, cuando el primer procedimiento 213 de aplicación en el modo de seguridad corresponde al servicio de correo, el primer procedimiento 213 de aplicación en el modo de seguridad genera una dirección para almacenar datos de correo en un área de seguridad preestablecida de la memoria 105 a través de un procedimiento diferente de aquel en el que un el procedimiento del servicio de correo recibe y genera una dirección para almacenar los datos del correo recibido.

Esto también es igualmente aplicable a un procedimiento 212 de descarga en el modo de seguridad. Es decir, a diferencia de un procedimiento de descarga de datos en el modo sin seguridad, el procedimiento 212 de descarga en el modo de seguridad incluye un módulo de cifrado para cifrar los datos recibidos y un proxy para inducir el cifrado. Además, el procedimiento de generar la dirección para almacenar los datos cifrados puede ser diferente de un procedimiento en el que el procedimiento de descarga en el modo sin seguridad genera una dirección.

Mientras tanto, cuando se genera un evento particular para proporcionar un mensaje de notificación, como la recepción de correo, en un procedimiento correspondiente, el procedimiento 212 de descarga en el modo de seguridad, el primer procedimiento 213, ... de aplicación en el modo de seguridad y un procedimiento 214 de aplicación en el modo de seguridad de orden m proporcionan el evento generado al procedimiento 221 de proxy de notificación en el modo de seguridad incluido dentro del procedimiento 220 de mensaje de notificación. En este momento, un mensaje generado para informar sobre el evento puede tener un formulario diferente al de una notificación de evento en el modo sin seguridad. Es decir, cierta información, como un tipo del evento generado, se informa y la información detallada sobre el evento generado no se proporciona. Por ejemplo, cuando un correo corresponde al evento recibido, el procedimiento de aplicación correspondiente informa al procedimiento 221 de proxy de notificación en el modo de seguridad solo de la recepción del correo y no informa de un remitente ni del asunto del correo. Es decir, cuando se genera un evento particular, todos los procedimientos en el modo de seguridad pueden configurarse para proporcionar solo la generación del evento correspondiente al procedimiento 221 de proxy de notificación en el modo de seguridad.

A continuación, el procedimiento 221 de proxy de notificación en el modo de seguridad muestra directamente el mensaje correspondiente cuando un modo actual es el modo de seguridad. En algunas implementaciones, el procedimiento 221 de proxy de notificación de seguridad puede informar sobre el tipo de evento generado independientemente del modo actual. Esto se describirá con referencia a la Figura 3.

La Figura 3 ilustra un ejemplo de visualización de un mensaje de notificación en el modo sin seguridad y un mensaje de notificación en el modo de seguridad en la unidad de visualización del dispositivo electrónico de acuerdo con las realizaciones de la presente invención.

Como se ilustra en la Figura 3, el procedimiento 220 de mensaje de notificación o/y el procedimiento 221 de proxy de notificación en el modo de seguridad se controlan para mostrar la existencia del mensaje de notificación en un área para informar la generación de un evento particular a través de un procedimiento predeterminado. Por ejemplo, cuando se supone que el dispositivo electrónico es un terminal que proporciona una entrada del usuario en un tipo de pantalla táctil, el usuario puede tocar la unidad 106 de visualización para desplazarse hacia abajo para identificar los mensajes de notificación a través del tipo de pantalla táctil como lo indica el número 311 de referencia. De acuerdo con el desplazamiento hacia abajo, los mensajes se muestran como indicados con los números 321 y 322 de referencia.

El área 301 para informar sobre la generación del evento particular de acuerdo con la presente invención puede ser al menos una parte de todas las áreas del dispositivo electrónico, así como un área ilustrada en la Figura 3.

La Figura 3 ilustra un caso en el que un procedimiento de aplicación de correo en el modo sin seguridad recibe un correo y un procedimiento de aplicación de correo en el modo seguro recibe tres correos. Un orden de recibir los correos puede corresponder a uno de los siguientes cuatro ordenes.

1. Recibir correo en el modo sin seguridad -> recibir primer correo en el modo de seguridad -> recibir segundo correo en el modo de seguridad -> recibir tercer correo en el modo de seguridad
2. Recibir el primer correo en el modo de seguridad -> recibir el correo en el modo sin seguridad -> recibir el segundo correo en el modo de seguridad -> recibir el tercer correo en el modo de seguridad
3. Recibir el primer correo en el modo de seguridad -> recibir el segundo correo en el modo de seguridad -> recibir el correo en el modo sin seguridad -> recibir el tercer correo en el modo de seguridad
4. Recibir el primer correo en el modo de seguridad -> recibir el segundo correo en el modo de seguridad -> recibir el tercer correo en el modo de seguridad -> recibir el correo en el modo sin seguridad

De acuerdo con la presente invención, se puede aplicar cualquiera de los cuatro ordenes anteriores. Además, la información de notificación de correos recibidos de acuerdo con los cuatro ordenes puede almacenarse secuencialmente en una pila predeterminada (no mostrada).

De acuerdo con las realizaciones de la presente invención, en el caso del correo en el modo sin seguridad, el procedimiento 220 de mensaje de notificación puede mostrar la recepción de un correo (un correo electrónico ha llegado), un remitente del correo (de: Mathew (m.nilson@gmail.com)) y un asunto (Asunto: Oye, ¿vienes este fin de semana?) en la unidad 106 de visualización como se indica con el número 321 de referencia.

Además, de acuerdo con las realizaciones de la presente invención, en un caso del correo en el modo de seguridad, el procedimiento 221 de proxy de notificación en el modo de seguridad del procedimiento 220 de mensaje de notificación muestra una indicación (3 mensajes de correo electrónico sin leer en el modo de seguridad) simplemente indicando que tres correos se han recibido en el modo de seguridad en la unidad 106 de visualización como se indica con el número 322 de referencia. En algunas implementaciones, cuando un modo actual es el modo de seguridad, el procedimiento de 221 de proxy de notificación en el modo de seguridad puede mostrar información detallada del mensaje correspondiente como se indica mediante el número 321 de referencia.

Como se ilustra en la Figura 3, el mensaje de notificación de los procedimientos en el modo sin seguridad puede configurarse básicamente para mostrar todos los contenidos detallados. En otro procedimiento para mostrar el mensaje de notificación mediante los procedimientos en el modo sin seguridad, el mensaje puede informarse como se indica por el número 321 de referencia solo en el modo sin seguridad y solo se informa el número de mensajes como se indica mediante el número 322 de referencia en el modo de seguridad.

Se supone que un estado en que se muestra el mensaje de notificación como se ilustra en la Figura 3 corresponde al modo sin seguridad. En el modo sin seguridad, el usuario selecciona una ventana 322 de notificación de correo en el modo de seguridad. En este caso, el procedimiento 215 de gestión en el modo de seguridad identifica un archivo de política almacenado previamente. Cuando no se permite un acceso, el procedimiento 215 de gestión en el modo de seguridad controla para mostrar un mensaje que informa de la negación del acceso en la unidad 106 de visualización como se ilustra en la Figura 4A o 4B.

Un asunto que identifica el archivo de política almacenado previamente puede ser el procedimiento 215 de gestión en el modo de seguridad o puede existir un procedimiento separado para identificar si se permite el acceso. Además, en ambos casos en que hay un procedimiento separado y el procedimiento 215 de gestión en el modo de seguridad decide si se permite el acceso, se realiza una función correspondiente cuando el acceso está permitido y un mensaje que informa que el acceso no está permitido se muestra en la unidad 106 de visualización cuando el acceso no está permitido.

Las Figuras 4A y 4B ilustran ejemplos de pantallas para describir casos en los que se requiere acceso a un modo configurado actualmente y otro modo y se deniega el acceso de acuerdo con la presente invención.

En la Figura 4A, un mensaje 410 emergente de negación simple para informar simplemente que el acceso está denegado se visualiza en la unidad 106 de visualización. En otro procedimiento, en la pantalla 106 de la Figura 4B se muestra un mensaje 420 emergente de negación de consulta compleja para proporcionar una consulta adicional para preguntar al usuario si se debe mostrar continuamente un mensaje de negación junto con la negación del acceso.

En el mensaje 420 emergente de negación de consulta compleja, se muestran los iconos 421 y 422 de selección para identificar si se acepta la negación del acceso y un icono 423 de consulta para preguntar sobre un tipo de permiso de acceso posterior. Como se ilustra en la Figura 4B, los iconos 421 y 422 de selección para identificar si aceptar la negación pueden configurarse para haber seleccionado Sí 421 cuando se acepta la negación y para haber seleccionado No 422 cuando la negación no se acepta.

Además, en el mensaje 420 emergente de negación de consulta compleja, se puede incluir el icono 423 de consulta sobre el tipo de permiso de acceso posterior. El tipo de permiso de acceso ilustrado en la Figura 4B puede incluir los siguientes cuatro tipos.

1. "No ver esta advertencia...»
2. "Bloquear solo este caso"
3. "Solo registro"
4. "Desactivar esta advertencia"

Cuando se deben agregar diversos casos adicionales de los permisos de acceso a los tipos de permisos de acceso mencionados anteriormente, se pueden agregar otros casos. Cuando hay tipos de permisos de acceso innecesarios en los tipos de permisos de acceso enumerados anteriormente, los tipos de permisos de acceso correspondientes se pueden eliminar para reducir el número de casos.

Basándose en la descripción anterior, se describirá un procedimiento para proporcionar información en el modo de seguridad en el modo sin seguridad.

Cuando se genera un evento que da importancia a la transferencia en tiempo real en el modo de seguridad mientras el usuario usa el dispositivo electrónico en el modo sin seguridad, cada uno de los procedimientos en el modo de seguridad proporciona información mínima sobre el evento generado al procedimiento 220 de mensaje de notificación o al procedimiento de 221 de proxy de notificación en el modo de seguridad.

A continuación, el procedimiento 220 de mensaje de notificación o el procedimiento 221 de proxy de notificación en el modo de seguridad reciben la información del evento correspondiente y envía los datos recibidos a través de la unidad 106 de visualización. En consecuencia, un mensaje en el modo de seguridad que da importancia a la transferencia en tiempo real puede identificarse también en el modo sin seguridad.

A continuación, de acuerdo con la descripción anterior, se describirá un procedimiento para cambiar un procedimiento del tratamiento cuando se viola una política de seguridad en el modo sin seguridad.

Un procedimiento o un servicio correspondiente a un asunto que procesa una operación de acuerdo con si se viola la política de seguridad en el modo sin seguridad puede configurarse por un dominio al que se debe acceder por adelantado, es decir, si se utiliza el modo de seguridad o el modo sin seguridad. La configuración puede almacenarse en un archivo predeterminado o recibirse de un dispositivo externo como un servidor.

Cada uno de los asuntos tiene una etiqueta que define una autoridad de acceso para un objeto que el asunto desea usar, es decir, un archivo o una carpeta, y la etiqueta puede comprimir o convertirse en un archivo de política y luego almacenarse en un área predeterminada de la memoria 105.

Por consiguiente, el objeto establecido a ser utilizado en el modo de seguridad, por ejemplo, una Base de Datos (DB), un archivo, una carpeta, y/o una aplicación puede accederse por un procedimiento o servicio particular o el usuario en el modo de seguridad. En este caso, el procedimiento 215 de gestión en el modo de seguridad para gestionar el acceso detecta una acción de infracción de acceso con referencia al archivo de política.

En consecuencia, cuando un procedimiento particular viola una política, el procedimiento 215 de gestión en el modo de seguridad controla para mostrar un mensaje 410 emergente de negación simple o un mensaje 420 emergente de negación de consulta compleja en la unidad 106 de visualización de acuerdo con un modo establecido. Las realizaciones de la presente invención incluyen los siguientes seis modos.

1. Notificación de uso del Modo 1 Obligatorio: prohibir contundentemente las infracciones e informar cada violación
2. Notificación de uso del Modo 2 Obligatorio: prohibir contundentemente las infracciones y no informar
3. Notificación de uso del Modo 3 Obligatorio: prohibir contundentemente solo este comportamiento
4. Notificación de uso del Modo 1 Permisivo: informar al usuario pero no prohibir contundentemente
5. Notificación de uso del Modo 2 Permisivo: no informar al usuario y solo realizar el registro
6. Notificación de uso del Modo 3 Permisivo: ninguna acción

Con la salida de los mensajes emergentes enumerados anteriormente, también se puede utilizar un sonido, una vibración y/o transmisión de un mensaje que informa a otro dispositivo electrónico, como un servidor, de la situación correspondiente.

La Figura 5 es una vista que describe operaciones de procedimientos cuando el dispositivo electrónico que tiene el modo de seguridad y el modo sin seguridad descarga una aplicación en el modo de seguridad e instala la aplicación descargada en el modo de seguridad de acuerdo con las realizaciones de la presente invención.

Cuando se ejecuta el procedimiento 211 de la tienda de aplicaciones en el modo de seguridad, el procedimiento 211 de la tienda de aplicaciones en el modo de seguridad ejecuta el procedimiento 201 de la tienda de aplicaciones en el modo sin seguridad en la etapa 500. En este momento, puesto que el procedimiento 201 de la tienda de aplicaciones en el modo sin seguridad se requiere para acceder a una tienda de aplicaciones mediante el procedimiento 211 de la tienda de aplicaciones en el modo de seguridad, el procedimiento 201 de la tienda de aplicaciones en el modo sin seguridad controla el módulo 110 de comunicación para acceder a un servidor que tiene una aplicación para el modo de seguridad en la tienda de aplicaciones, recibe una lista de aplicaciones de seguridad que se pueden instalar y muestra información de la lista recibida en la unidad 106 de visualización en la etapa 502.

Cuando se requiere que se instale una aplicación de seguridad particular, es decir, cuando se requiere que una aplicación de seguridad predeterminada se descargue e instale mediante un comando del usuario o un servidor particular, el procedimiento 201 de la tienda de aplicaciones controla el módulo 110 de comunicación para recibir el aplicación de seguridad del servidor correspondiente y proporciona la aplicación de seguridad recibida para el procedimiento 205 del agente de gestión en la etapa 504.

Cuando todos los datos de la aplicación que se instalarán se reciben del servidor que tiene la aplicación de seguridad, el procedimiento 205 del agente de gestión puede solicitar la instalación mientras proporciona los datos de la aplicación que se instalarán en el procedimiento 215 de gestión en el modo de seguridad existente en el modo de seguridad en la operación 506.

En consecuencia, el procedimiento 215 de gestión en el modo de seguridad instala la aplicación a través de la etapa 508 para generar un nuevo procedimiento 216 de aplicación en el modo de seguridad. Posteriormente, el procedimiento 215 de gestión en el modo de seguridad informa al usuario que la aplicación se ha instalado. Cuando el modo de usuario es el modo que no es de seguridad, el procedimiento 215 de gestión en el modo de seguridad proporciona solo información que informa que la aplicación se ha instalado en el procedimiento 220 de mensaje de notificación o el procedimiento de 221 de proxy de notificación en el modo de seguridad. En consecuencia, el procedimiento 220 de mensaje de notificación o el procedimiento 221 de proxy de notificación en el modo de seguridad pueden mostrar una indicación de que el procedimiento se ha instalado en la unidad 106 de visualización.

La Figura 6 ilustra un ejemplo que describe un procedimiento de visualización cuando el dispositivo electrónico que tiene el modo sin seguridad y el modo de seguridad comparte una interfaz independientemente del modo de acuerdo con las realizaciones de la presente invención.

Los procedimientos ilustrados en la Figura 6 permiten que las funciones utilizadas tanto en el modo de seguridad como en el modo sin seguridad muestren una interfaz ficticia en la unidad 106 de visualización en el modo de seguridad y las operaciones reales son realizadas por los procedimientos en el modo sin seguridad.

En consecuencia, un primer procedimiento 611 ficticio y un segundo procedimiento 612 ficticio en el modo de seguridad corresponden a interfaces ficticias y pueden ser procedimientos que realizan solo una operación para llamar a procedimientos que operan en el modo sin seguridad. Es decir, el primer procedimiento 611 ficticio es un procedimiento ficticio para llamar a un primer procedimiento 601 ficticio correspondiente y el segundo procedimiento 612 ficticio es un procedimiento para llamar a un segundo procedimiento 602 ficticio correspondiente.

El primer procedimiento 601 ficticio correspondiente y el segundo procedimiento 602 ficticio correspondiente realizan una operación real. Los procedimientos pueden ser, por ejemplo, un proceso de contacto, un proceso de calendario, un proceso de portapapeles, un proceso de registro del tratamiento de llamadas, un proceso de marcado, un proceso de mensaje (SMS/MMS) o similares.

El procedimiento ficticio corresponde a un puente unidireccional para una conexión del procedimiento en el modo sin seguridad y puede configurarse para funcionar solo cuando se intenta utilizar una función en el modo sin seguridad en el modo de seguridad. Además, cuando el usuario ejecuta el procedimiento correspondiente, el procedimiento ficticio se configura para realizar una función en el modo sin seguridad llamando al procedimiento correspondiente proporcionado en el modo sin seguridad a través del puente. En este momento, el procedimiento ficticio puede configurarse para usar una base de datos incluida solo en el modo de seguridad mientras realiza la función en el modo sin seguridad, según sea necesario.

Después, cada uno de los procedimientos mencionados anteriormente se describirá con más detalle. El procedimiento de contacto solo proporciona información básica, como un número de teléfono, un nombre y un grupo cuando el procedimiento ficticio llama al procedimiento de contacto. En consecuencia, se puede cargar información como una marcación rápida, una identificación con foto y un perfil, y la privacidad del usuario puede quedar protegida en el modo de seguridad. Además, cuando el procedimiento ficticio en el modo de seguridad llama al procedimiento de contacto, puede ser imposible editar los datos leídos de la base de datos.

El procedimiento de calendario se configura para leer solo información básica, como un asunto y la hora en que se comparten los datos correspondientes. El portapapeles realiza la misma operación tanto en el modo de seguridad como en el modo sin seguridad. Sin embargo, los datos almacenados en el portapapeles en el modo sin seguridad no pueden leerse en el modo de seguridad y los datos almacenados en el portapapeles en el modo de seguridad pueden no leerse en el modo sin seguridad.

El procedimiento de registro del tratamiento de llamadas lee la información de registro de una llamada saliente y una llamada entrante desde una base 621 de datos de registro del tratamiento de llamadas por igual en el modo de seguridad y en el modo sin seguridad. En la Figura 6, se supone que el segundo procedimiento 612 ficticio y el segundo procedimiento 602 ficticio correspondiente son un procedimiento ficticio del tratamiento de llamadas y un procedimiento correspondiente del tratamiento de llamadas, respectivamente.

Además, el procedimiento de marcado se configura para realizar una marcación por igual en el modo de seguridad, así como en el modo sin seguridad.

Un procedimiento 622 de alarma funciona igualmente en el modo de seguridad así como en el modo sin seguridad. Por consiguiente, como se ilustra en la Figura 6, puesto que no hay ningún asunto relacionado con la seguridad, el procedimiento ficticio no se puede utilizar.

La Figura 7 ilustra el dispositivo electrónico de acuerdo con las realizaciones de la presente invención.

Con referencia a la Figura 7, el dispositivo electrónico de acuerdo con una realización de la presente invención incluye un módulo 701 de reconocimiento de notificación, un módulo 702 de notificación, un módulo 703 de control de acceso y un procesador 700.

El dispositivo electrónico de acuerdo con una realización de la presente invención puede funcionar en uno de una pluralidad de modos de operación que incluyen un primer modo de operación y un segundo modo de operación. Por ejemplo, el primer modo de operación puede ser un modo configurado para cifrar datos y almacenar los datos cifrados en un área de memoria que está separada de los otros modos de operación restantes (por ejemplo, segundo modo de operación) y asignado al primer modo de operación, para permitir que solo un usuario autenticado acceda a los datos almacenados en el área de memoria asignada al primer modo de operación.

El módulo 701 de reconocimiento de notificación genera información de notificación para reconocer la información de notificación de un primer procedimiento de modo activado en el primer modo de operación de la pluralidad de modos de operación.

Por ejemplo, al menos una parte o la totalidad del módulo 701 de reconocimiento de notificación pueden incluirse en el procedimiento del primer modo que tiene la información de notificación generada.

El módulo 702 de notificación se configura para proporcionar una notificación al usuario del dispositivo electrónico basándose en una parte de la información de notificación generada en el módulo 701 de reconocimiento de notificación cuando un modo de operación actual no es el primer modo de operación. Por ejemplo, la parte de la información de notificación notificada por el módulo 702 de notificación puede incluir al menos una de si la información de notificación ha sido generada, un tipo de información de notificación generada, un número de veces que la información de notificación ha sido generada, y una cantidad de datos incluidos en la información de notificación.

Por ejemplo, al menos una parte o la totalidad del módulo 702 de notificación pueden incluirse en el procedimiento del primer modo que tiene la información de notificación generada.

El módulo 702 de notificación se configura para procesar una parte de la información de notificación en varios tipos y transmitir la información de notificación procesada al usuario. Por ejemplo, la parte de la información de notificación puede mostrarse en al menos una parte de una pantalla de visualización del dispositivo electrónico. Además, la notificación se puede proporcionar al usuario en varios tipos, como un sonido de notificación y una vibración de notificación, así como una notificación visual de este tipo. El módulo de notificación de acuerdo con la presente invención no limita un procedimiento de notificación en sí mismo.

El procesador 700 ejecuta al menos uno del módulo 701 de reconocimiento de notificación y el módulo 702 de notificación.

Cuando se detecta una solicitud de acceso para que los recursos configurados sean accesibles solo en el primer modo de operación, el módulo 703 de control de acceso se configura para bloquear la solicitud de acceso si el modo de operación actual no es el primer modo de operación.

En algunas implementaciones, el módulo 703 de control de acceso puede configurarse para mostrar un mensaje que indica que la solicitud de acceso ha sido bloqueada en la pantalla de visualización del dispositivo electrónico.

En algunas implementaciones, el módulo 703 de control de acceso puede configurarse para proporcionar un procedimiento de autenticación para acceder al primer modo de operación y permitir la solicitud de acceso del usuario si el usuario correspondiente tiene éxito en la autenticación de acuerdo con el procedimiento de autenticación proporcionado.

la Figura 8 es un diagrama de flujo de un procedimiento de notificación de información limitada de acuerdo con las realizaciones de la presente invención. El dispositivo electrónico que realiza el procedimiento corresponde al dispositivo electrónico ilustrado en la Figura 7.

Con referencia a la Figura 8, en la etapa 801, el procesador 700 del dispositivo electrónico ejecuta el módulo 701 de reconocimiento de notificación para reconocer la generación de la información de notificación del primer procedimiento de operación activado en el primer modo de operación de la pluralidad de modos de operación.

En la etapa 802, el procesador 700 del dispositivo electrónico ejecuta el módulo 702 de notificación para dar una notificación al usuario basándose en una parte de la información de notificación generada en el procedimiento del primer modo de operación si la operación actual no es el primer modo de operación.

En la etapa 802, el procesador 700 procesa una parte de la información de notificación en varios tipos y transmite la información de notificación procesada al usuario. Por ejemplo, la parte de la información de notificación puede mostrarse en al menos una parte de una pantalla de visualización del dispositivo electrónico. Además, la notificación se puede proporcionar al usuario en varios tipos, como un sonido de notificación y una vibración de notificación, así como una notificación visual de este tipo. El módulo de notificación de acuerdo con la presente invención no limita un procedimiento de notificación.

Cada una de las operaciones descritas en esta memoria descriptiva puede procesarse a través de un procedimiento secuencial, paralelo, repetitivo o heurístico y algunas de las operaciones pueden omitirse u otras operaciones pueden agregarse.

El procedimiento de acuerdo con la presente invención tal como se ha descrito anteriormente puede implementarse como un comando de programa que puede ejecutarse a través de varios ordenadores y grabarse en un medio de grabación legible por ordenador. El medio de grabación puede incluir un comando de programa, un archivo de datos y una estructura de datos. El comando del programa puede estar especialmente diseñado y configurado para la presente invención o puede usarse después de ser conocido por los expertos en campos de software informático. El medio de grabación puede incluir medios magnéticos como un disco duro, un disquete y una cinta magnética, medios ópticos como una memoria de solo lectura de disco compacto (CD-ROM) y un disco versátil digital (DVD), medios magnetoópticos como un disco floptical y dispositivos de hardware como una memoria de solo lectura (ROM), una memoria de acceso aleatorio (RAM) y una memoria flash. Además, el comando de programa puede incluir un código de lenguaje de máquina generado por un compilador y un código de lenguaje de alto nivel ejecutable por un ordenador a través de un intérprete y similares. Los dispositivos de hardware pueden configurarse para funcionar como uno o más módulos de software para realizar la presente invención.

Cada uno de los módulos desvelados en esta memoria descriptiva puede configurarse mediante software, firmware, hardware o una combinación de los mismos. Además, algunos de los módulos pueden combinarse como un módulo u omitirse. Cuando se combinan, las funciones que han sido realizadas por los módulos correspondientes antes de la combinación pueden realizarse igualmente.

Aplicabilidad industrial

De acuerdo con las realizaciones desveladas en esta memoria descriptiva, las realizaciones de prevención pueden aplicar dispositivos electrónicos que tienen el modo de seguridad y un modo sin seguridad.

Texto libre de lista de secuencias

101 : unidad de radio
102 : módem
103 : unidad de cámara
105 : memoria
106 : Unidad de visualización
107 : unidad de entrada
110: módulo de comunicación
ANT: antena
201 : procedimiento de la tienda de aplicaciones
202 : primer procedimiento de aplicación
203 : segundo procedimiento de aplicación
204 : procedimiento de aplicación de orden n
205 : procedimiento del agente de gestión
211 : procedimiento de la tienda de aplicaciones en el modo de seguridad
212 : procedimiento de descarga en el modo de seguridad
213 : primer procedimiento de aplicación en el modo de seguridad
214 : procedimiento de aplicación de modo de seguridad de orden m
215 : procedimiento de gestión en el modo de seguridad
220 : procedimiento de mensaje de notificación
221 : procedimiento de proxy de notificación en el modo de seguridad
601 : primer procedimiento ficticio correspondiente
602 : segundo procedimiento ficticio correspondiente
611 : primer procedimiento ficticio
612 : segundo procedimiento ficticio
621 : base de datos de registro del tratamiento de llamadas
622 : procedimiento de alarma
700 : procesador
701 : módulo de reconocimiento de notificación
702 : módulo de notificación
703 : módulo de control de acceso

REIVINDICACIONES

1. Un procedimiento de control de información utilizando un dispositivo electrónico, comprendiendo el procedimiento:

reconocer (801) la generación de información de notificación de uno o más procedimientos activados en un primer modo de operación entre una pluralidad de modos de operación que incluyen el primer modo de operación y un segundo modo de operación; y
notificar (802) a un usuario de solo una parte de la información de notificación cuando un modo de operación actual es el segundo modo de operación,
caracterizado porque la parte de la información de notificación proporciona menos información que la información de notificación, y la información de notificación incluye al menos un número de veces que la información de notificación se ha generado para el usuario.

2. El procedimiento de la reivindicación 1, en el que la parte de la información de notificación incluye al menos una de si se ha generado o no la información de notificación, un tipo de información de notificación y una cantidad de datos incluidos en la información de notificación.

3. El procedimiento de la reivindicación 1, en el que la parte de la información de notificación corresponde a una parte de los datos que se mostrarán al usuario de acuerdo con la información de notificación cuando el modo de operación actual es el primer modo de operación.

4. El procedimiento de la reivindicación 1, en el que notificar al usuario la parte de la información de notificación comprende:
transmitir al menos una parte de la información de notificación a un segundo procedimiento que recopila la información de notificación del primer modo de operación mediante un primer procedimiento que genera la información de notificación; y notificar al usuario la parte de la información de notificación mediante el segundo procedimiento.

5. El procedimiento de la reivindicación 1, en el que notificar al usuario la parte de la información de notificación comprende mostrar al menos una parte de la información de notificación en al menos una parte de una pantalla (106) de visualización del dispositivo electrónico.

6. El procedimiento de la reivindicación 1, en el que el primer modo de operación cifra datos y almacena los datos cifrados en un área de memoria separada del segundo modo de operación y asignada al primer modo de operación, y en el que solo un usuario autenticado puede acceder a datos almacenados en el área de memoria asignada al primer modo de operación.

7. El procedimiento de la reivindicación 1, que además comprende:

detectar una solicitud de acceso a recursos configurados para ser accesibles solo en el primer modo de operación; y
Bloquear la solicitud de acceso cuando el modo de operación actual no es el primer modo de operación.

8. El procedimiento de la reivindicación 7, en el que bloquear la solicitud de acceso comprende mostrar un mensaje (420) que indica que la solicitud de acceso está bloqueada en una pantalla (106) de visualización del dispositivo electrónico.

9. El procedimiento de la reivindicación 7, que además comprende:

proporcionar un procedimiento de autenticación para acceder el primer modo de operación al usuario; y
permitir la solicitud de acceso cuando el usuario tiene éxito en una autenticación a través del procedimiento de autenticación proporcionado.

10. Un dispositivo electrónico que comprende:

un módulo (701) de reconocimiento configurado para reconocer (801) la generación de información de notificación de uno o más procedimientos activados en un primer modo de operación entre una pluralidad de modos de operación que incluyen el primer modo de operación y un segundo modo de operación; y
un módulo (702) de notificación configurado para notificar (802) a un usuario de solo una parte de la información de notificación cuando un modo de operación actual es el segundo modo de operación
caracterizado porque la parte de la información de notificación proporciona menos información que la información de notificación, y la información de notificación incluye al menos un número de veces que la información de notificación se ha generado para el usuario.

11. El dispositivo electrónico de la reivindicación 10, en el que el uno o más procedimientos incluyen al menos una parte del módulo (701) de reconocimiento o al menos una parte del módulo (801) de notificación.

12. El dispositivo electrónico de la reivindicación 10, en el que la parte de la información de notificación incluye al menos una de si se ha generado o no la información de notificación, un tipo de información de notificación y una cantidad de datos incluidos en la información de notificación.

13. El dispositivo electrónico de la reivindicación 10, en el que la parte de la información de notificación corresponde a una parte de los datos que se mostrarán al usuario de acuerdo con la información de notificación cuando el modo de operación actual es el primer modo de operación.

14. El dispositivo electrónico de la reivindicación 10, en el que el módulo de notificación recibe al menos una parte de la información de notificación mediante un procedimiento que tiene la información de notificación generada y notifica al usuario la parte recibida de la información de notificación.

15. El dispositivo electrónico de la reivindicación 10, en el que el módulo de notificación muestra una parte de la información de notificación en al menos una parte de un área de una pantalla (106) de visualización del dispositivo electrónico.

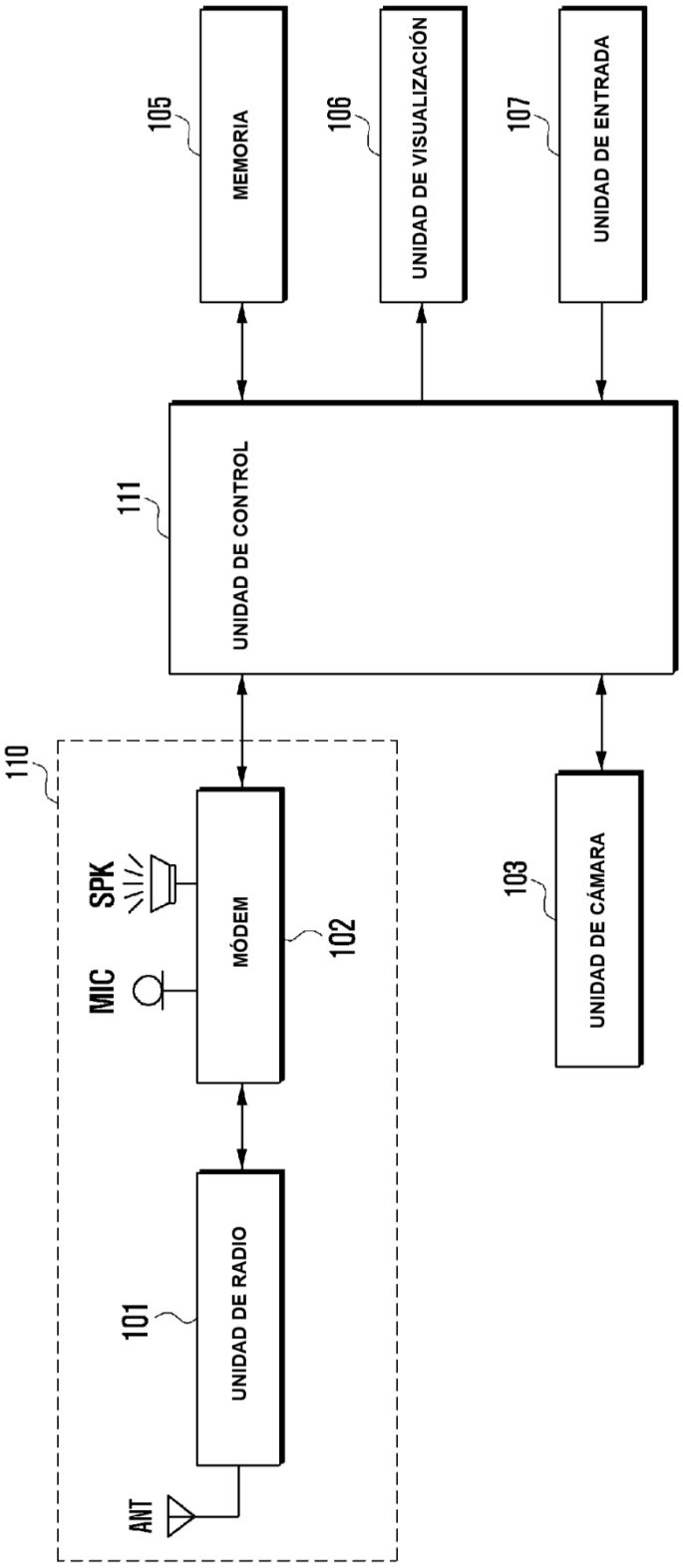
16. El dispositivo electrónico de la reivindicación 10, en el que el primer modo de operación cifra datos y almacena los datos cifrados en un área de memoria que está separada del segundo modo de operación y asignada al primer modo de operación, y
en el que solo un usuario autenticado puede acceder a los datos almacenados en el área de memoria asignada al primer modo de operación.

17. El dispositivo electrónico de la reivindicación 10, que comprende además, cuando se detecta una solicitud de acceso recursos configurados para ser solo accesibles en el primer modo de operación, un módulo (703) de control de acceso que se configura para bloquear la solicitud de acceso si el modo de operación actual no es el primer modo de operación.

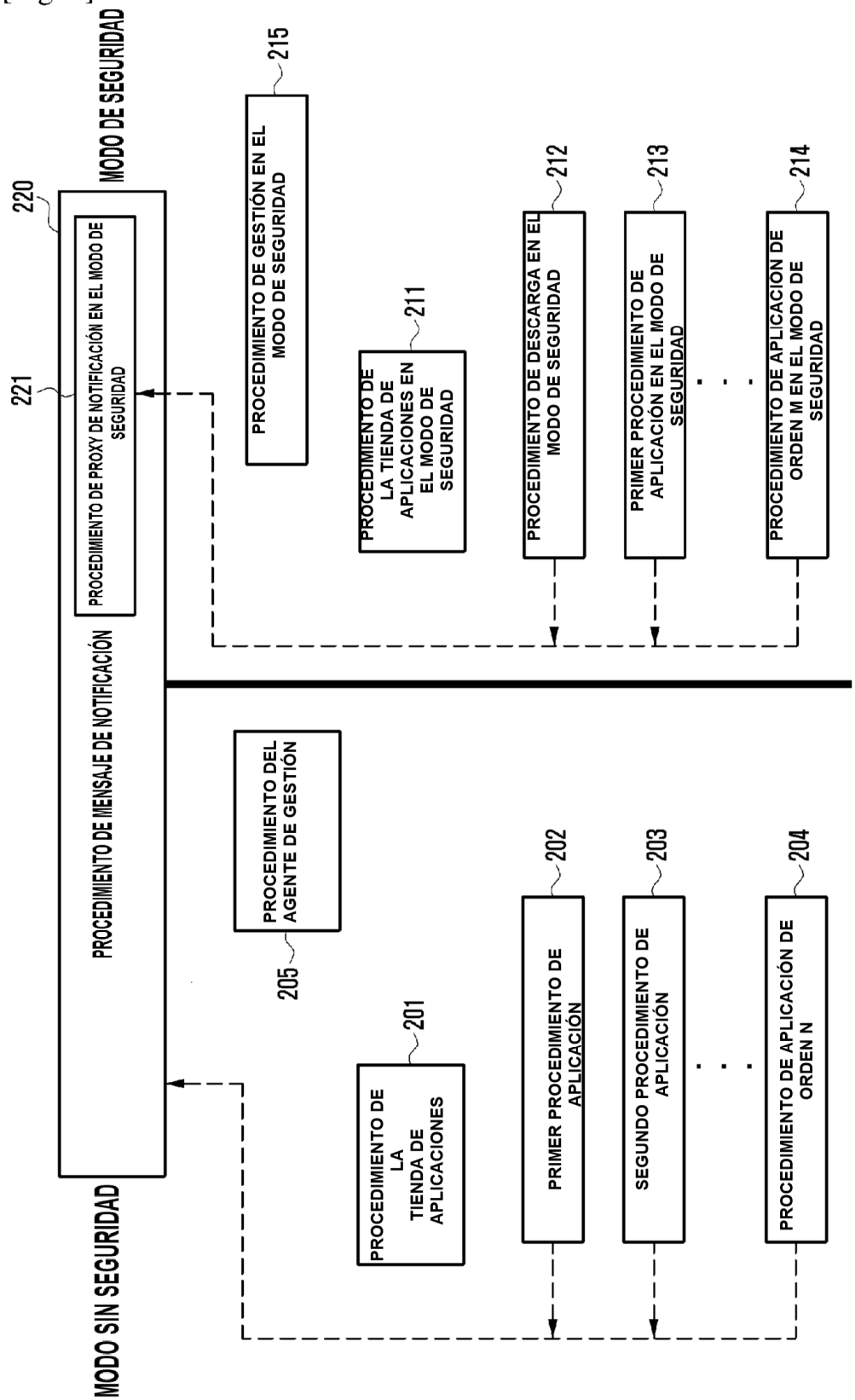
18. Un medio (105) de almacenamiento que comprende comandos que, cuando son ejecutados por un dispositivo electrónico, hacen que el dispositivo lleve a cabo las operaciones que comprenden:

reconocer (801) la generación de información de notificación de uno o más procedimientos activados en un primer modo de operación entre una pluralidad de modos de operación que incluyen el primer modo de operación y un segundo modo de operación; y
notificar (802) a un usuario de solo una parte de la información de notificación cuando un modo de operación actual es el segundo modo de operación,
caracterizado porque la parte de la información de notificación proporciona menos información que la información de notificación, y la información de notificación incluye al menos un número de veces que la información de notificación se ha generado para el usuario.

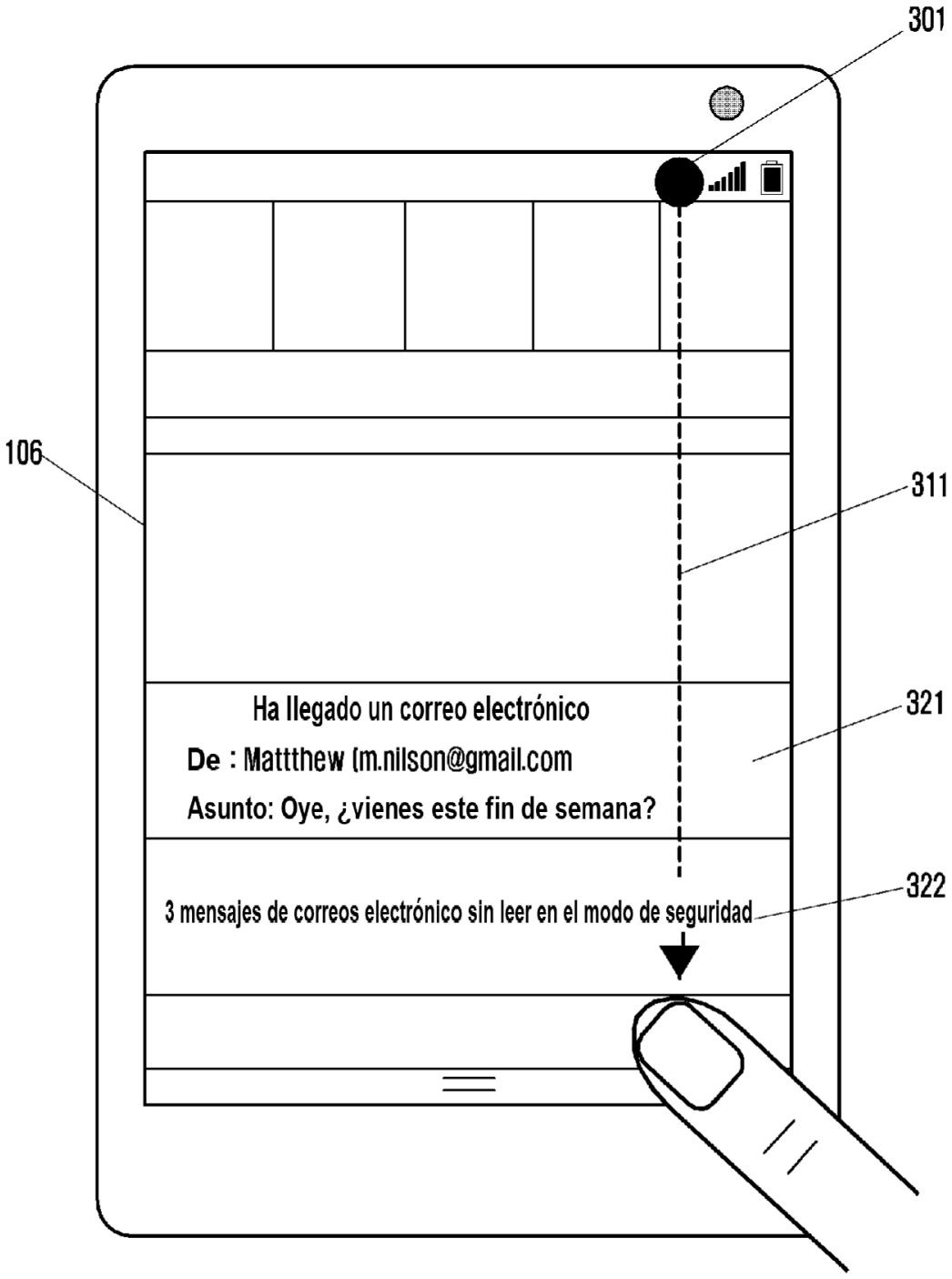
[Fig. 1]


105
MEMORIA
106
UNIDAD DE VISUALIZACIÓN
107
UNIDAD DE ENTRADA
111
UNIDAD DE CONTROL
110
SPK
MIC
MÓDEM
102
103
UNIDAD DE CÁMARA
101
UNIDAD DE RADIO
ANT

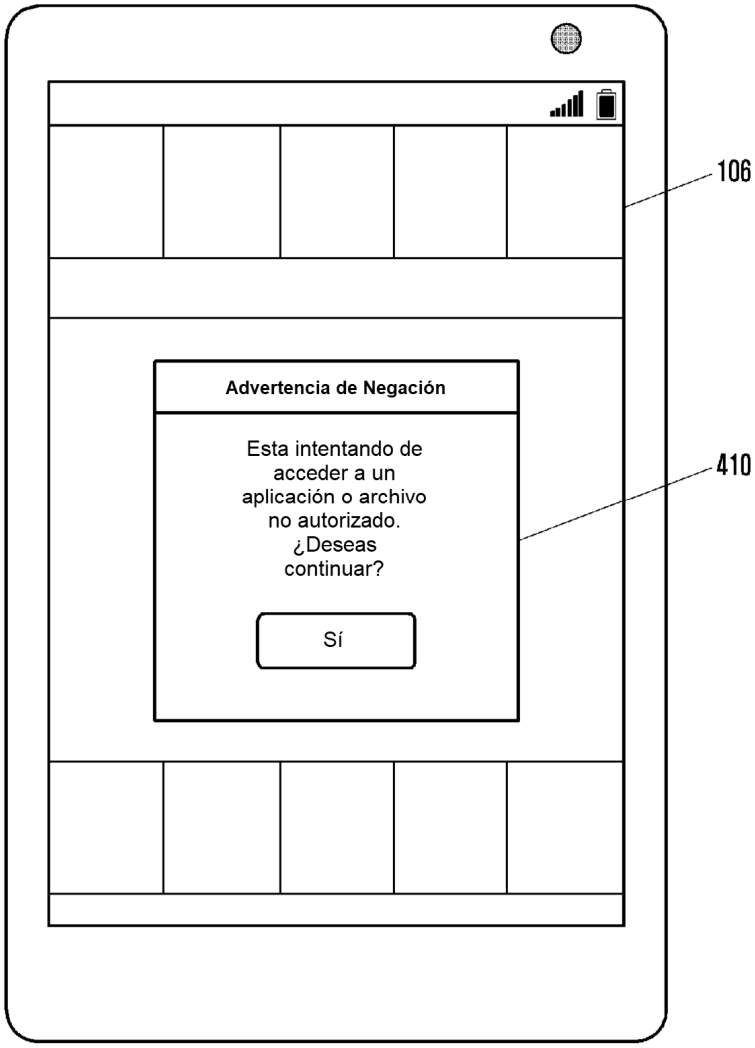
[Fig. 2]


MODO DE SEGURIDAD
220
221
PROCEDIMIENTO DE PROXY DE NOTIFICACIÓN EN EL MODO DE SEGURIDAD
PROCEDIMIENTO DE MENSAJE DE NOTIFICACIÓN
MODO SIN SEGURIDAD
215
PROCEDIMIENTO DE GESTIÓN EN EL MODO DE SEGURIDAD
211
PROCEDIMIENTO DE LA TIENDA DE APLICACIONES EN EL MODO DE SEGURIDAD
212
PROCEDIMIENTO DE DESCARGA EN EL MODO DE SEGURIDAD
213
PRIMER PROCEDIMIENTO DE APLICACIÓN EN EL MODO DE SEGURIDAD
214
PROCEDIMIENTO DE APLICACION DE ORDEN M EN EL MODO DE SEGURIDAD
205
PROCEDIMIENTO DEL AGENTE DE GESTIÓN
201
PROCEDIMIENTO DE LA TIENDA DE APLICACIONES
202
PRIMER PROCEDIMIENTO DE APLICACIÓN
203
SEGUNDO PROCEDIMIENTO DE APLICACIÓN
204
PROCEDIMIENTO DE APLICACIÓN DE ORDEN N

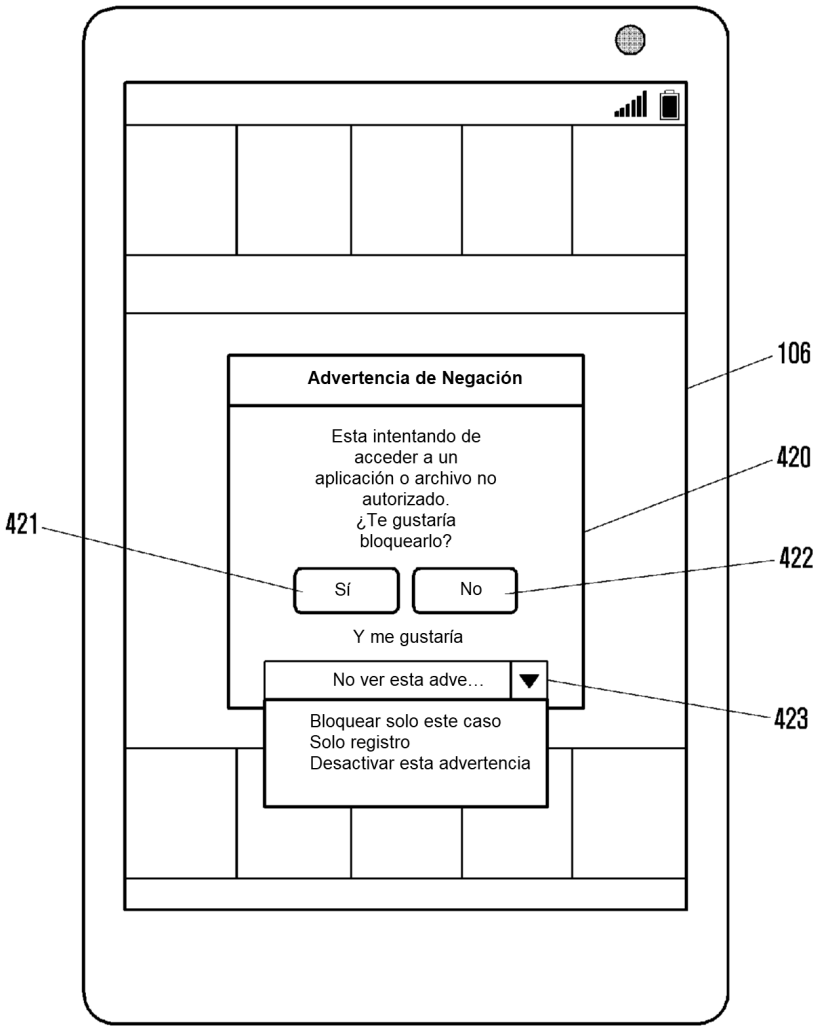
[Fig. 3]


301
106
311
321
322
Ha llegado un correo electrónico
De : Mattthew (m.nilson@gmail.com
Asunto: Oye, ¿vienes este fin de semana?
3 mensajes de correos electrónico sin leer en el modo de seguridad

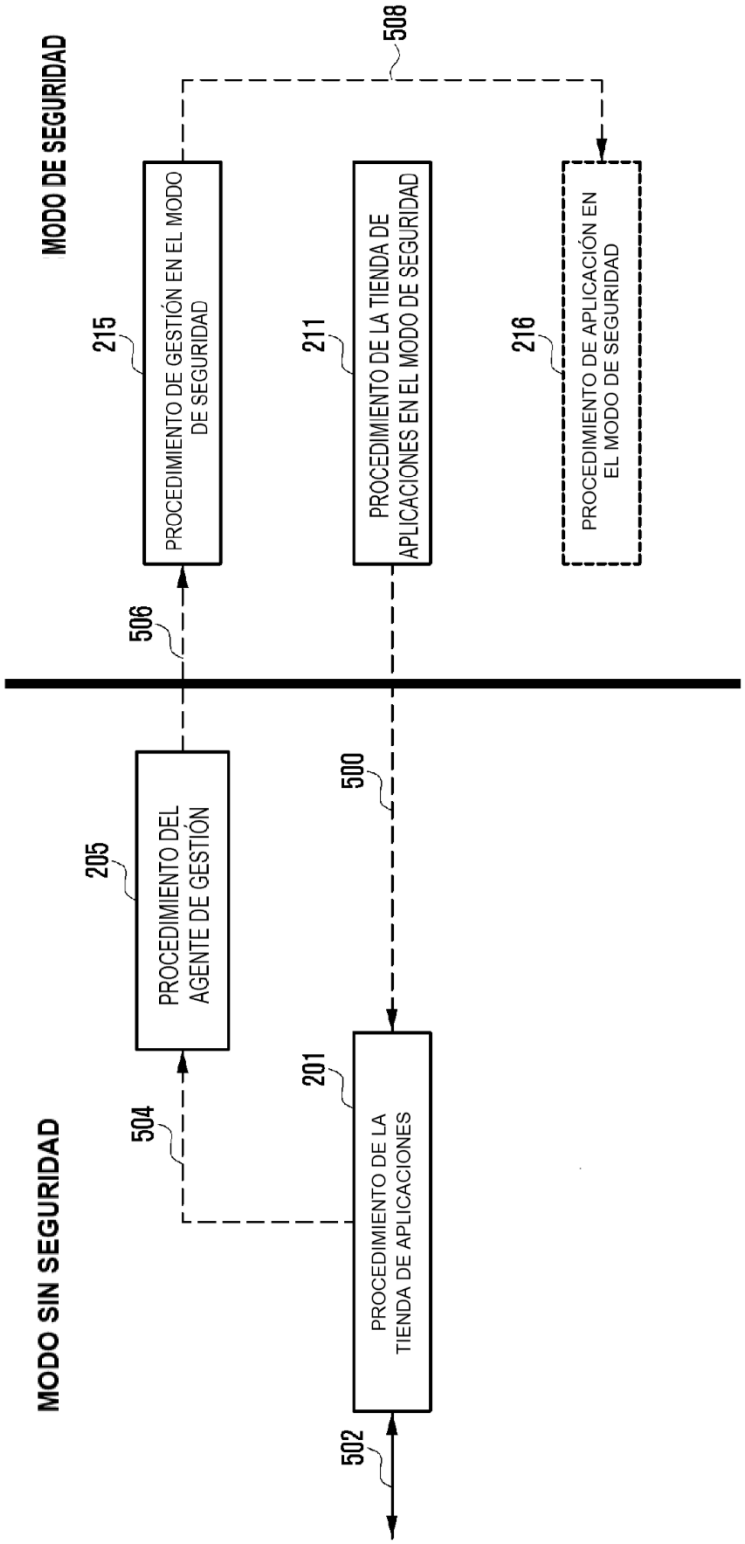
[Fig. 4a]


106
Advertencia de Negación
Esta intentando de acceder a un aplicación o archivo no autorizado. ¿Deseas continuar?
Sí
410

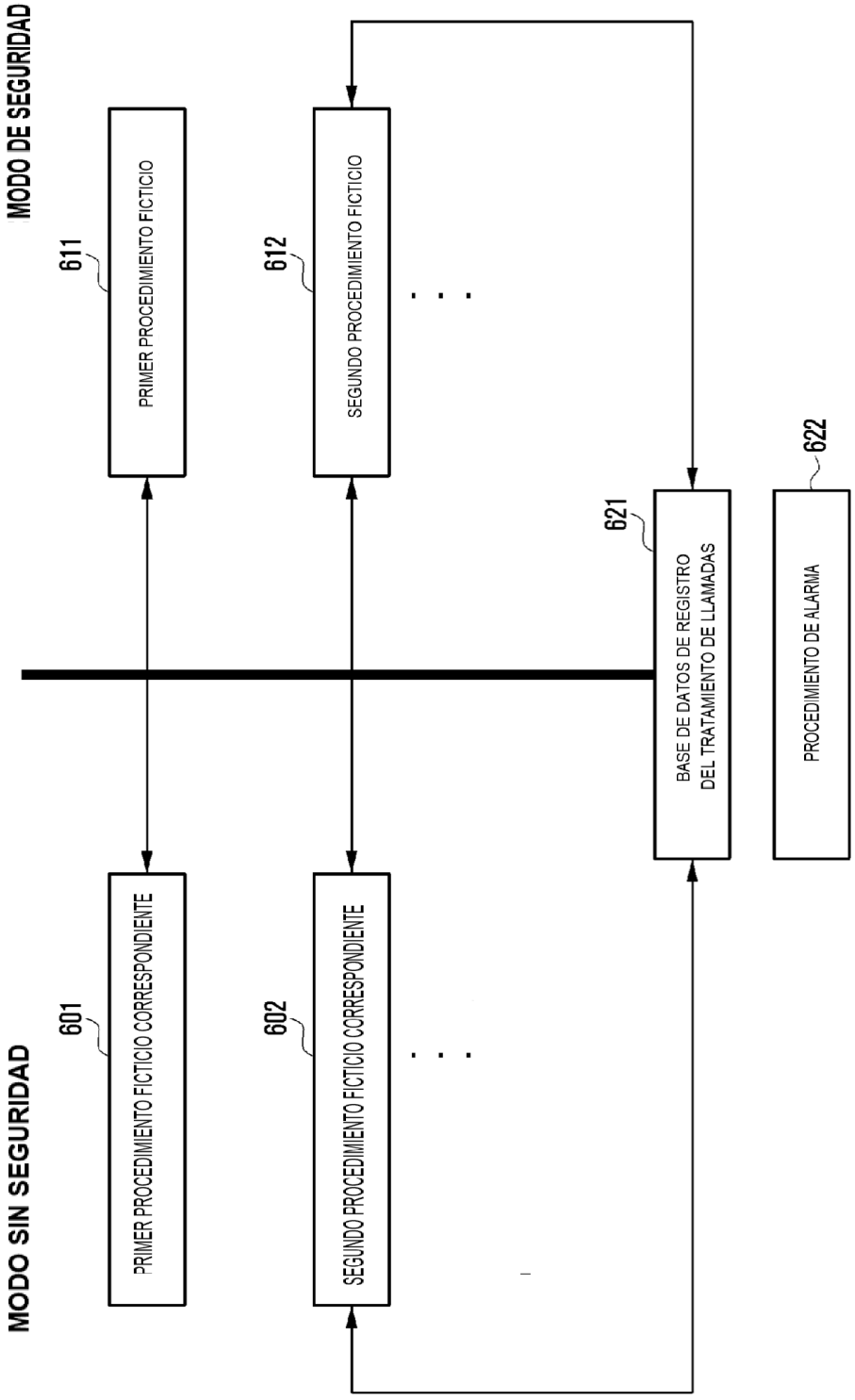
[Fig. 4b]


Advertencia de Negación
Esta intentando de acceder a un aplicación o archivo no autorizado. ¿Te gustaría bloquearlo?
Sí
No
Y me gustaría
No ver esta adve…
Bloquear solo este caso
Solo registro
Desactivar esta advertencia
106
420
421
422
423

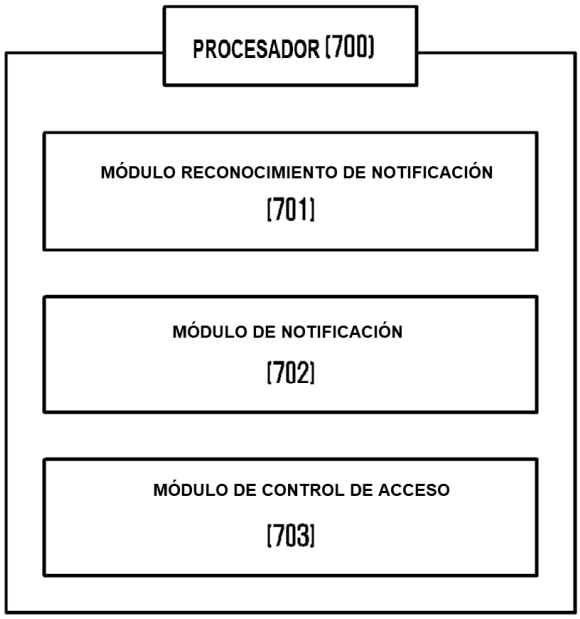
[Fig. 5]


MODO DE SEGURIDAD
MODO SIN SEGURIDAD
508
215
PROCEDIMIENTO DE GESTIÓN EN EL MODO DE SEGURIDAD
211
PROCEDIMIENTO DE LA TIENDA DE APLICACIONES EN EL MODO DE SEGURIDAD
216
PROCEDIMIENTO DE APLICACIÓN EN EL MODO DE SEGURIDAD
506
205
PROCEDIMIENTO DEL AGENTE DE GESTIÓN
500
504
201
PROCEDIMIENTO DE LA TIENDA DE APLICACIONES
502

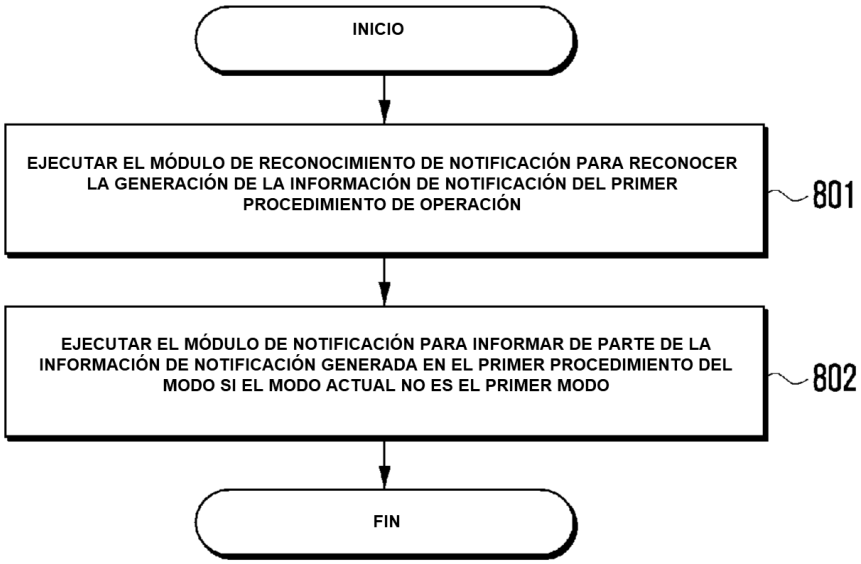
[Fig. 6]


MODO DE SEGURIDAD
611
PRIMER PROCEDIMIENTO FICTICIO
612
SEGUNDO PROCEDIMIENTO FICTICIO
621
BASE DE DATOS DE REGISTRO DEL TRATAMIENTO DE LLAMADAS
622
PROCEDIMIENTO DE ALARMA
MODO SIN SEGURIDAD
601
PRIMER PROCEDIMIENTO FICTICIO CORRESPONDIENTE
602
SEGUNDO PROCEDIMIENTO FICTICIO CORRESPONDIENTE

[Fig. 7]


PROCESADOR (700)
MÓDULO RECONOCIMIENTO DE NOTIFICACIÓN
(701)
MÓDULO DE NOTIFICACIÓN
(702)
MÓDULO DE CONTROL DE ACCESO
(703)

[Fig. 8]


INICIO
EJECUTAR EL MÓDULO DE RECONOCIMIENTO DE NOTIFICACIÓN PARA RECONOCER LA GENERACIÓN DE LA INFORMACIÓN DE NOTIFICACIÓN DEL PRIMER PROCEDIMIENTO DE OPERACIÓN
801
EJECUTAR EL MÓDULO DE NOTIFICACIÓN PARA INFORMAR DE PARTE DE LA INFORMACIÓN DE NOTIFICACIÓN GENERADA EN EL PRIMER PROCEDIMIENTO DEL MODO SI EL MODO ACTUAL NO ES EL PRIMER MODO
802
FIN