(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 462 398**

(21) Número de solicitud: 201231602

(51) Int. CI.:

H04L 9/00 (2006.01)

(12) SOLICITUD DE PATENTE A1

(22) Fecha de presentación:

18.10.2012

(43) Fecha de publicación de la solicitud:

22.05.2014

(56) Se remite a la solicitud internacional:

PCT/ES2013/070687

(71) Solicitantes:

NAVISTA S.A.R.L. (100.0%)
567 RUE FELIX TROMBE
PERPIGNAN FR

(72) Inventor/es:

VINEGLA, Jean;
BIAL, Emmanuel T.A.;
LECLERCQ, Jean Noel G. y
PINSON, Jean Marc R.

(74) Agente/Representante:

GUTIERREZ HERNANDEZ, Francisco

(54) Título: **MÉTODO PARA LIMITAR Y ASEGURAR LA OPERATIVIDAD Y FUNCIONAMIENTO DE UN PROGRAMA DE ORDENADOR ÚNICA Y EXCLUSIVAMENTE CON EL EQUIPO INFORMÁTICO DONDE SE INSTALA**

(57) Resumen:

Método para limitar y asegurar la operatividad y funcionamiento de un programa de ordenador única y exclusivamente con el equipo informático particular donde se instala, que, durante la instalación del software en el equipo, comprende un proceso de escaneo del hardware presente, identificando los parámetros que son únicos en él para conseguir la "firma ADN del hardware" con la que se genera una clave K1 con la que se encriptan en un documento de datos cifrado informaciones importantes de acceso al programa, y luego se borran la clave K1 y los datos de dichas informaciones de acceso al programa, y solo se guarda el documento cifrado.

ES 2 462 398 A1

DESCRIPCIÓN

Método para limitar y asegurar la operatividad y funcionamiento de un programa de ordenador única y exclusivamente con el equipo informático donde se instala

OBJETO DE LA INVENCIÓN

La invención, tal como expresa el enunciado de la presente memoria descriptiva, se refiere a un método para limitar y asegurar la operatividad y funcionamiento de un programa de ordenador, única y exclusivamente con el equipo informático donde se instala.

Más en particular, el objeto de la invención se centra en un sistema de seguridad informático que, tiene como finalidad hacer que un programa de ordenador o software opere y funcione solamente con el equipo informático o dispositivo electrónico concreto en el que se instala. Con ello se consigue que dicho software solo pueda trabajar con dicho equipo en particular y no en ningún otro, evitando así cualquier posibilidad de que, por razones de seguridad o en caso de robo, copia, u otra acción se pueda llevar a cabo el uso no autorizado de dicho software.

Para ello, el método propuesto comprende una serie de fase de implementación que asegura que dicho software solo funcionará con el hardware presente durante la fase de instalación del software en el equipo. Asimismo, el método propuesto contempla otra fase que asegura que dicho software para funcionar en dicho equipo usa una clave encriptada y, finalmente, una fase que asegura que dicha clave encriptada solo es utilizable si se cumple lo expuesto en la primera fase de implementación, es decir, que el hardware sea estrictamente el mismo, con los mismos elementos y componentes concretos que los que estaban presentes durante la fase de instalación del software.

CAMPO DE APLICACIÓN DE LA INVENCIÓN

El campo de aplicación de la presente invención se enmarca dentro del sector de la informática, centrándose en el ámbito de la seguridad en el uso de software o programas informáticos, aplicaciones informáticas, etc.

ANTECEDENTES DE LA INVENCIÓN

En la actualidad, y como referencia al estado de la técnica, cabe mencionar que, se conocen diferentes sistema de protección para evitar el uso no autorizado de programas informáticos.

Sin embargo, la mayoría de dichos sistemas se centran en introducir en el propio programa elementos de protección para evitar su copia, por ejemplo el uso de contraseñas, claves identificativas, códigos, etc., que tarde o temprano siempre son susceptibles de ser descubiertos y/o falseados por "*hackers"* informáticos u otros especialistas.

Por ello, en los sistemas hasta ahora conocidos, una vez salvados los obstáculos de seguridad que se introducen en el programa, este puede ser tranquilamente usado en cualquier otro equipo en el que se reinstale, con la sola condición de que dicho equipo cuente con el hardware necesario para ello, lo cual evidencia que los sistemas existentes adolecen de la suficiente garantía para muchos sectores de la industria y el comercio.

Por ello, el objetivo de la presente invención es desarrollar un innovador sistema de protección informático cuyo objetivo es ir más allá de la simple protección del software en sí y alcanzar la protección del conjunto software-equipo, de tal forma que dicho software solo pueda funcionar con el equipo informático, dispositivo o aparato para el que esté instalado y autorizado y en ninguno más, aunque disponga de idéntico hardware.

Es decir, la solución que propone la presente invención a la problemática que plantean los sistemas existentes es conseguir asegurar que un software instalado en un equipo esté vinculado al mismo de manera única y no se pueda separar del hardware concreto y particular de dicho equipo para hacerlo funcionar en otro equipo o aparato.

Así, si se produce un robo del software, éste no podrá funcionar de manera separada al hardware al que se hubo vinculado durante la instalación del mismo.

Cabe señalar además que, al menos por parte del solicitante, se desconoce la existencia de ningún otro método para limitar y asegurar la operatividad y funcionamiento de un programa de ordenador, única y exclusivamente con el equipo informático en particular donde se instala, ni de ninguna otra invención de aplicación similar ni que presente unas características técnicas y constitutivas semejantes o equivalentes a las que presenta el método aquí preconizado, según se reivindica.

EXPLICACIÓN DE LA INVENCIÓN

Así, el método para limitar y asegurar la operatividad y funcionamiento de un programa de ordenador, única y exclusivamente con el equipo informático donde se instala, que la presente invención propone, se configura como una destacable novedad dentro de su campo de aplicación, ya que, a tenor de su implementación y de forma taxativa se alcanzan satisfactoriamente los objetivos anteriormente señalados, estando los detalles caracterizadores que lo hacen posible convenientemente recogidos en las reivindicaciones finales que acompañan a la presente memoria descriptiva.

De forma concreta, y como ya se ha apuntado anteriormente, lo que la invención propone es un sistema de seguridad informático mediante el cual, un determinado software, entendiendo el término "software" como programa de ordenador, programa informático o aplicación programada para realizar tareas específicas en una computadora, solamente funciona con el equipo informático concreto, único y particular en el que se instala dicho software, entendiéndose que al hablar de equipo informático se pretende abarcar cualquier aparato, máquina o dispositivo electrónico capaz de hacer funcionar un software y que, por tanto, comprende un hardware o conjunto de elementos y componentes electrónicos, tales como CPU, memorias (RAM, ROM, HDD, Flash), y puertos de comunicación, etc.

Para ello, y de forma concreta, el método en cuestión, durante la instalación del software en el equipo, comprende las siguientes fases: Escaneo del hardware presente en dicho equipo durante dicha instalación, identificando los parámetros que son únicos en él para conseguir lo que denominaremos la "firma ADN del hardware" y que lo hace único y distinto a cualquier otro. Seguidamente y usando la descrita firma ADN del hardware obtenida como se ha descrito, así como una función matemática más un número fijo, se genera una clave. Dicha clave se utiliza para encriptar en un documento de datos cifrado algunas de las informaciones importantes de acceso que tenga el programa, tales como contraseñas, claves privadas, códigos de licencia, etc. Una vez encriptadas dichas informaciones, se borran tanto la clave como los datos de las informaciones de acceso al programa, y solo se guarda el documento cifrado.

Así, para poder usar el programa, para lo cual será necesario abrir el documento encirptado, éste solo podrá ser desencriptado volviendo a generarse la clave, la cual, a su vez, solo puede generarse usando la firma ADN del hardware del equipo, la cual solo se obtendrá si verdaderamente se trata del mismo equipo en el que se instaló el software, con el mismo hardware que estaba presente durante la instalación de dicho software en él.

El descrito método para limitar y asegurar la operatividad y funcionamiento de un programa de ordenador, única y exclusivamente con el equipo informático donde se instala representa, pues, una innovación de características estructurales y constitutivas desconocidas hasta ahora para el fin a que se destina, razones que unidas a su utilidad práctica, la dotan de fundamento suficiente para obtener el privilegio de exclusividad que se solicita.

DESCRIPCIÓN DE LAS FIGURAS

Para complementar la descripción que se está realizando y con objeto de ayudar a una mejor comprensión del método de la invención, se acompaña a la presente memoria descriptiva, como parte integrante de la misma, de un juego de figuras en las que se ha representado lo siguiente:

La figura número 1a y 1b muestran sendas partes de un diagrama de flujos que refleja la primera fase del método objeto de la invención en la que se contempla el proceso de obtención de la matriz inicial del equipo. En dichas partes las referencias (a) y (b) muestran la continuidad de las líneas de flujo entre ambas.

La figura número 2, es un diagrama de flujos que el proceso de obtención de la matriz final señalado en la segunda fase del método preconizado.

La figura número 3, es un diagrama de flujos que muestra la tercera fase del método que comprende el proceso de generación de la clave K1.

La figura número 4, es un diagrama de flujos que el proceso descrito en la fase cuatro del método de la invención, donde se encripta el documento con la información de accesibilidad al programa.

DESCRIPCIÓN DETALLADA DE LA INVENCIÓN

A la vista de los descritos diagramas, se observa cómo el método propuesto contempla una serie de fases de implementación del sistema de seguridad, las cuales se llevan a cabo durante el proceso de instalación del software en el equipo, y se describen detalladamente a continuación:

- Primera fase:

Durante la instalación del programa de ordenador en el equipo, el software de instalación de dicho programa está programado para que realice un examen de todo el hardware del equipo (procesador, puertos de comunicación, etc.) y pueda definir una serie de parámetros (tales como capacidad, frecuencia, dirección IP, ID de usuario, número de serie, tipo, marca, etc.) que sean constantes y únicos en dicho equipo. Ese conjunto de parámetros únicos y constantes determinarán lo que daremos en llamar “firma ADN del equipo”, ya que constituyen la firma identificativa que hace único a dicho equipo en particular.

Para conseguir dicha firma ADN se lleva a cabo un proceso repetitivo de examen de los parámetros citados, el cual genera n matrices con los datos obtenidos, con el objetivo de ir eliminando en ellas los parámetros que no se repitan y mantener solo los que siempre son idénticos y así generar una matriz inicial del equipo.(figuras 1-A y 1-B)

- Segunda fase:

Durante el proceso de implementación del sistema, lo aplicado en la primera fase al equipo se aplica paralelamente a un equipo similar de referencia, obteniéndose como resultado la creación de dos matrices: una matriz inicial o matriz 1, con los parámetros singulares del equipo en que se implementa el sistema; y una matriz de referencia o matriz 2, con los parámetros que tenga el hardware de dicho equipo de referencia. Todo ello con el fin de eliminar de la matriz inicial 1 todos aquellos parámetros que sean comunes también a esta matriz de referencia 2, y así obtener una matriz final o matriz F, con los parámetros que verdaderamente son únicos para el equipo, constituyendo la firma ADN identificativa del hardware del equipo (figura 2) .

- Tercera fase:

Tras la obtención de la firma ADN del hardware del equipo, el software de instalación genera una clave (que denominaremos clave K1) usando la firma ADN del hardware obtenida con la matriz final antedicha así como una fórmula encriptada (por ejemplo un algoritmo como HMAC-SHA 256) más un número fijo (figura 3).

- Cuarta fase:

Durante el proceso de implementación del sistema, algunas informaciones importantes de acceso al programa, tales como contraseñas, claves privadas RSD, códigos de licencia, etc., son encriptadas usando la citada clave K1, debiendo recordarse que dicha clave K1 está estrechamente relacionada con la firma ADN del hardware del equipo y, por tanto, solo es válida para dicho equipo.

Por último, se eliminan, tanto la base de datos que contiene las informaciones importantes de acceso como la clave K1, y en el equipo solo se conserva almacenado el documento encriptado con los datos de las informaciones importantes de acceso (figura 4).

Con todo ello queda implementado el sistema de seguridad que limita y asegura la operatividad y funcionamiento del programa de ordenador, única y exclusivamente con el equipo informático en particular donde ha sido instalado.

Al ir a usar el programa con el equipo donde está instalado, una vez implementado el sistema de seguridad en él, dicho programa lleva a cabo un proceso mediante el cual regenera la clave K1 recalculando la firma ADN del hardware. Con la clave K1 el equipo puede descifrar el documento encriptado del que precisará para acceder a la información que almacena y operar de forma normal, por ejemplo para abrir una conexión VPN (siglas del Inglés *Virtual Private Network*) con otro equipo.

De este modo, si por alguna razón se intentase abrir o utilizar o hacer funcionar el programa en cualquier otro equipo, aparato o dispositivo, al no cumplirse las condiciones para que pueda regenerar la clave K1, ya que la firma ADN del software de otro equipo no sería la misma, el programa no podrá desencriptar el documento que contiene la información de acceso y, por tanto, no funcionará. Además, al haberse borrado tanto los datos como la clave que abre el documento, éstos no podrán ser “haqueados”.

En definitiva y de manera concisa, el método para limitar y asegurar la operatividad y funcionamiento de un programa de ordenador, única y exclusivamente con el equipo informático en particular donde se instala, propuesto por la presente invención, comprende una fase de implementación que asegura que dicho software solo funcionará con el hardware presente durante la fase de instalación del software en el equipo, para lo cual, durante la instalación del software se lleva a cabo un proceso de escaneo del hardware del equipo para conseguir la firma ADN del mismo, identificando para ello los parámetros que están presentes y son únicos en él. Asimismo, el método propuesto contempla otra fase que asegura que dicho software para funcionar en dicho equipo usa una clave encriptada y que dicha clave encriptada solo es utilizable si se cumple lo expuesto en la primera fase de implementación, es decir, que el hardware sea estrictamente el mismo, con los mismos

elementos y componentes concretos que los que estaban presentes durante la fase de instalación del software, para ello, dicha clave se genera a partir de la firma ADN obtenida en la primera fase de implementación, con ella se encripta la información importante de acceso en un documento cerrado y se eliminan tanto dicha información como la clave, de tal forma que cada vez que se usa el programa éste ha de regenerar la clave a partir del ADN del equipo, asegurando así que solo funcionará con dicho equipo.

Descrita suficientemente la naturaleza de la presente invención, así como la manera de ponerla en práctica, no se considera necesario hacer más extensa su explicación para que cualquier experto en la materia comprenda su alcance y las ventajas que de ella se derivan, haciéndose constar que, dentro de su esencialidad, podrá ser llevada a la práctica en otras formas de realización que difieran en detalle de la indicada a título de ejemplo, y a las cuales alcanzará igualmente la protección que se recaba siempre que no se altere, cambie o modifique su principio fundamental.

Glosario de abreviaturas y términos utilizados.

CPU	- procesador
RAM	- memoria de acceso aleatorio
ROM	- memoria de sólo lectura
HDD	- unidad de disco duro
Memoria FLASH	- memoria volátil
clave RSA	- del inglés *Rivest-Shaiqir-Adleinan* algoritmo cifrado
DD	-unidad de disco
Puertos	- dispositivos de comunicación
S/N	- número de serie
HMAC-SHA256	-algoritmo de codificación
AES256	-Sistema Avanzado 256-bit de cifrar.

REIVINDICACIONES

1.- MÉTODO PARA LIMITAR Y ASEGURAR LA OPERATIVIDAD Y FUNCIONAMIENTO DE UN PROGRAMA DE ORDENADOR ÚNICA Y EXCLUSIVAMENTE CON EL EQUIPO INFORMÁTICO PARTICULAR DONDE SE INSTALA, **caracterizado** porque, durante la instalación del software en el equipo, comprende las siguientes fases:

- escaneo del hardware presente en dicho equipo durante dicha instalación, identificando los parámetros que son únicos en él para conseguir la “firma ADN del hardware” que lo hace único;

- usando la firma ADN del hardware obtenida, se genera una clave K1;

usando la citada clave K1, se encriptan en un documento de datos cifrado algunas informaciones importantes de acceso al programa, tales como contraseñas, claves privadas, códigos de licencia, etc.;

- luego, se borran la clave K1 y los datos con las informaciones de acceso al programa, y solo se guarda el documento cifrado con los datos de las citadas informaciones importantes de acceso, y que solo podrá ser desencriptado, para poder usar el programa, volviendo a generarse la clave K1, la cual, a su vez, solo puede generarse usando la firma ADN del hardware del equipo.

2.- MÉTODO PARA LIMITAR Y ASEGURAR LA OPERATIVIDAD Y FUNCIONAMIENTO DE UN PROGRAMA DE ORDENADOR ÚNICA Y EXCLUSIVAMENTE CON EL EQUIPO INFORMÁTICO PARTICULAR DONDE SE INSTALA, según la reivindicación 1, **caracterizado** porque, el proceso de escaneo del hardware presente en dicho equipo durante dicha instalación, para identificar los parámetros que son únicos en él y conseguir la “firma ADN del hardware” consiste en un examen de repetitivo de todo el hardware del equipo (procesador, puertos de comunicación, etc.) que define parámetros (tales como capacidad, frecuencia, dirección IP, ID de usuario, número de serie, tipo, marca, etc.), generando n matrices con los datos obtenidos para definir cuáles son constantes y únicos, y a partir de ellas generar una matriz inicial que se compara con una matriz de referencia obtenida mediante el mismo proceso repetitivo con un equipo de referencia similar dando lugar a una matriz final con los parámetros que verdaderamente son únicos para el equipo, y que constituyen la firma ADN identificativa del hardware del equipo.

3.- MÉTODO PARA LIMITAR Y ASEGURAR LA OPERATIVIDAD Y FUNCIONAMIENTO DE UN PROGRAMA DE ORDENADOR ÚNICA Y EXCLUSIVAMENTE CON EL EQUIPO INFORMÁTICO PARTICULAR DONDE SE INSTALA, según la reivindicación 1 ó 2, **caracterizado** porque la clave K1 que se genera usando la firma ADN del hardware, se genera usando además una fórmula encriptada más un número fijo.

4.- MÉTODO PARA LIMITAR Y ASEGURAR LA OPERATIVIDAD Y FUNCIONAMIENTO DE UN PROGRAMA DE ORDENADOR ÚNICA Y EXCLUSIVAMENTE CON EL EQUIPO INFORMÁTICO PARTICULAR DONDE SE INSTALA, según la reivindicación 3, **caracterizado** porque la fórmula encriptada que se usa junto al ADN del hardware para generar la clave K1 es un algoritmo como HMAC-SHA 256.

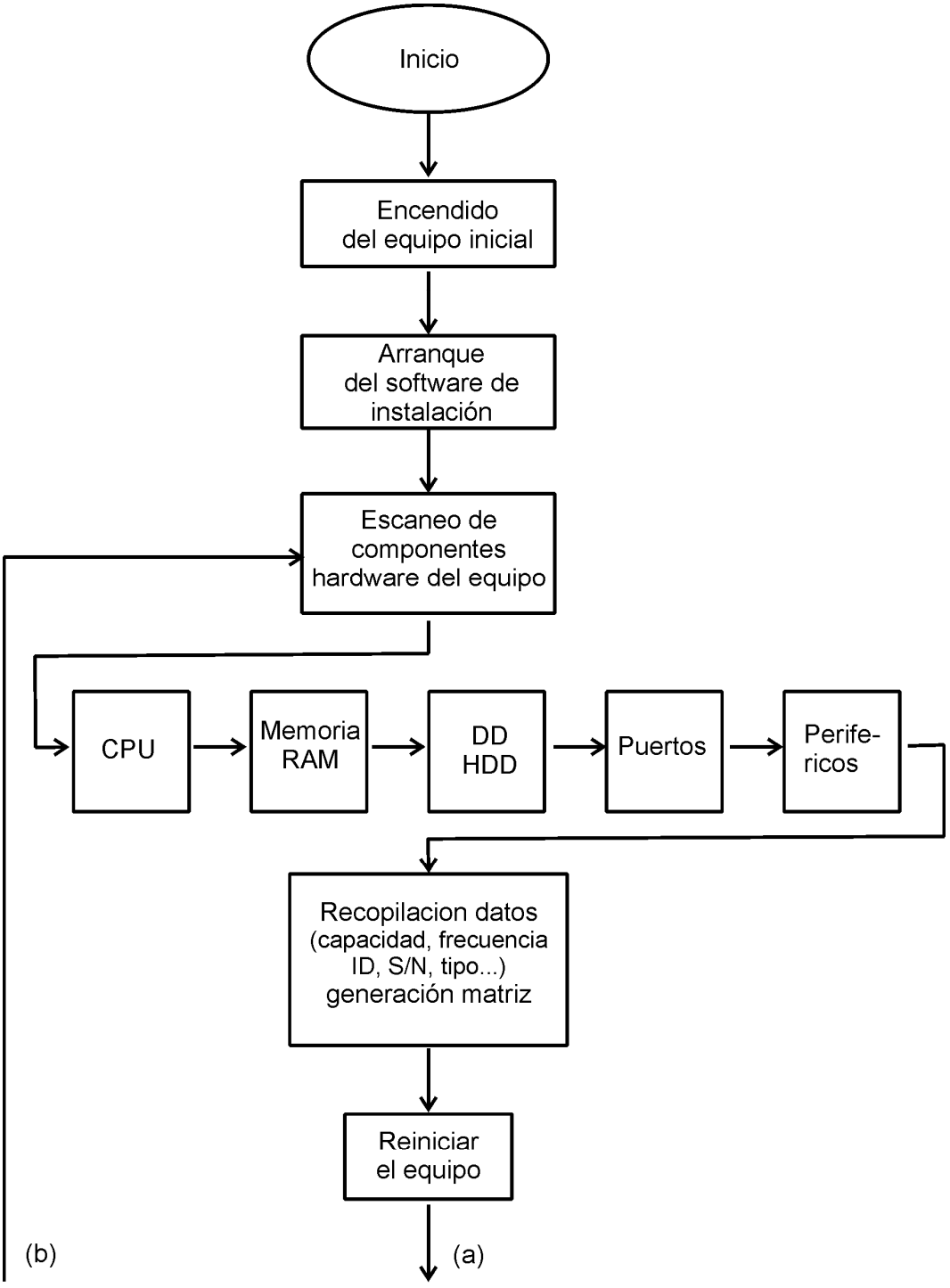
Inicio
Encendido del equipo inicial
Arranque del software de instalación
Escaneo de componentes hardware del equipo
CPU
Memoria RAM
DD HDD
Puertos
Perife-ricos
Recopilacion datos (capacidad, frecuencia ID, S/N, tipo...) generación matriz
Reiniciar el equipo
(b)
(a)

FIG. 1-A

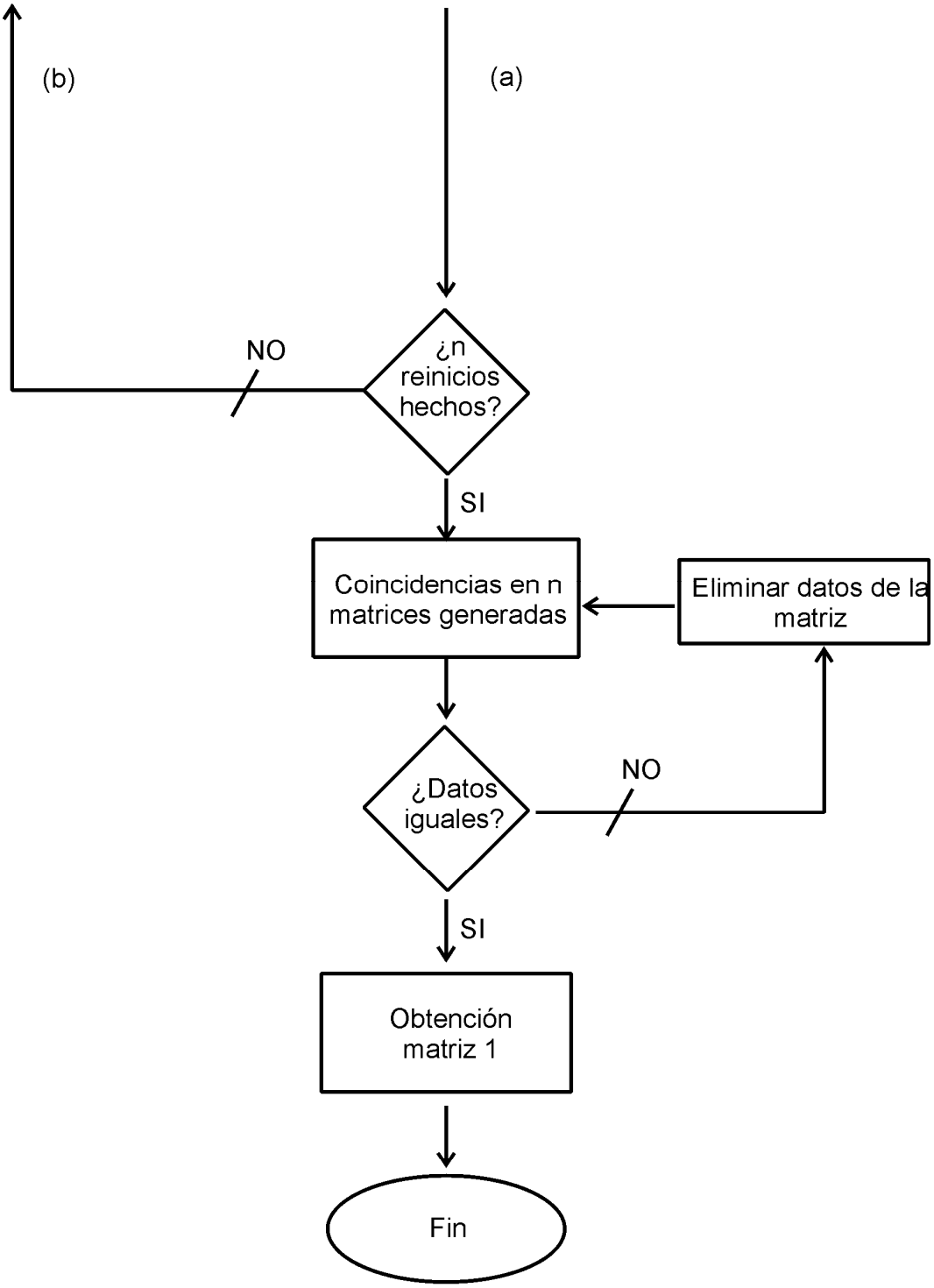
(b)
(a)
NO
¿n reinicios hechos?
SI
Coincidencias en n matrices generadas
Eliminar datos de la matriz
¿Datos iguales?
NO
SI
Obtención matriz 1
Fin

FIG. 1-B

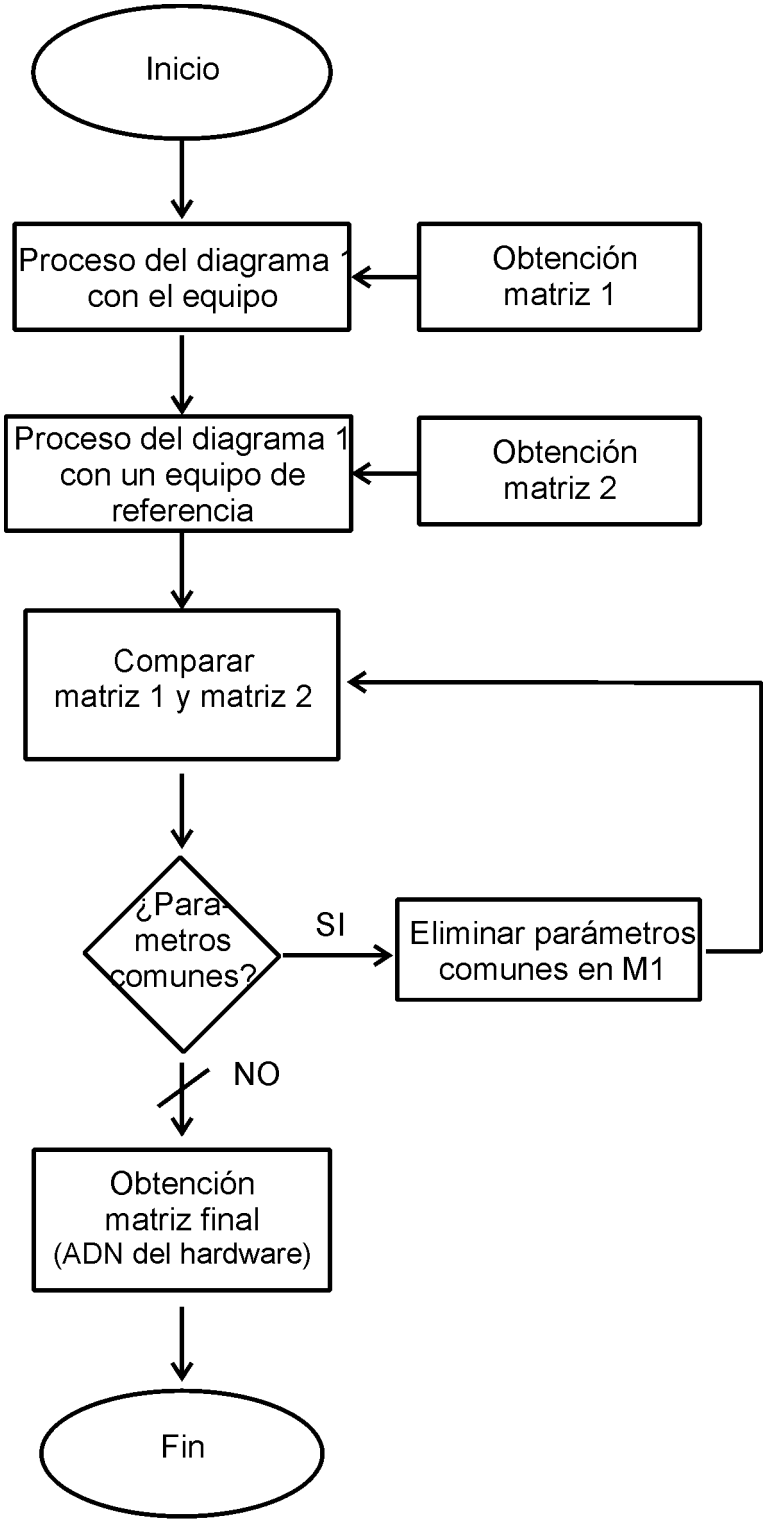
Inicio
Proceso del diagrama 1 con el equipo
Obtención matriz 1
Proceso del diagrama 1 con un equipo de referencia
Obtención matriz 2
Comparar matriz 1 y matriz 2
¿Parámetros comunes?
SI
Eliminar parámetros comunes en M1
NO
Obtención matriz final (ADN del hardware)
Fin

FIG. 2

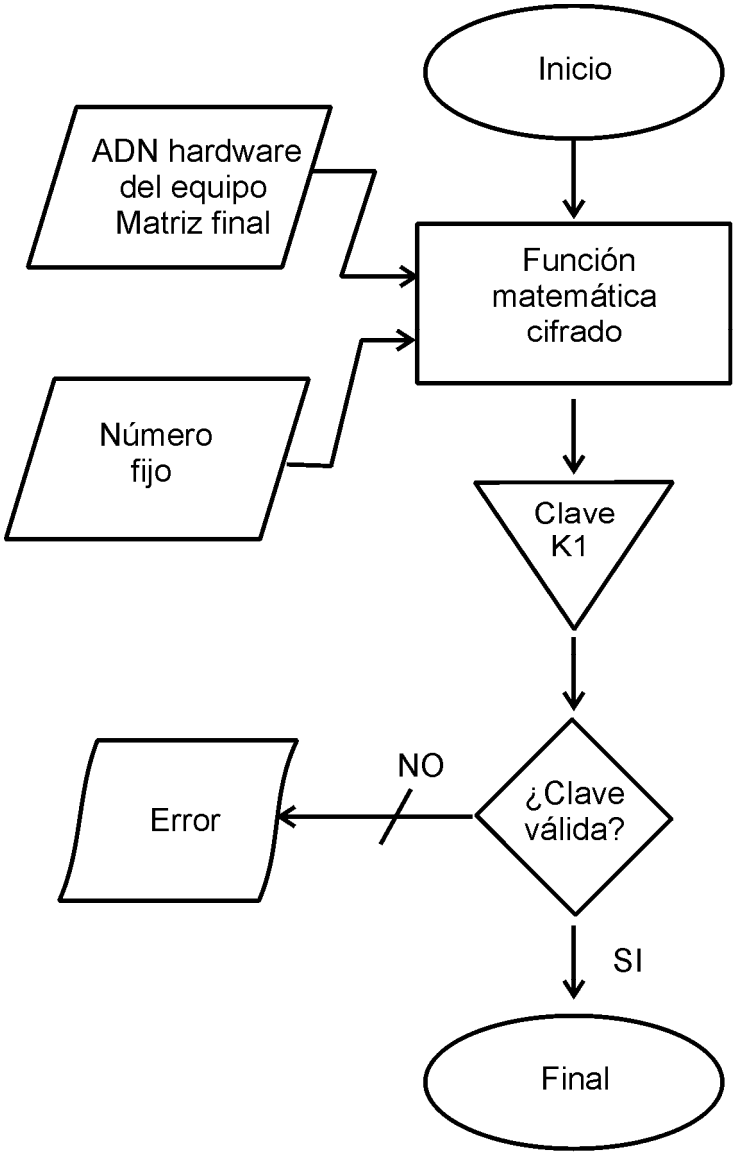
Inicio
ADN hardware del equipo Matriz final
Función matemática cifrado
Ejemplo: HMAC-SHA256
Número fijo
Clave K1
NO
Error
¿Clave válida?
SI
Final

FIG. 3

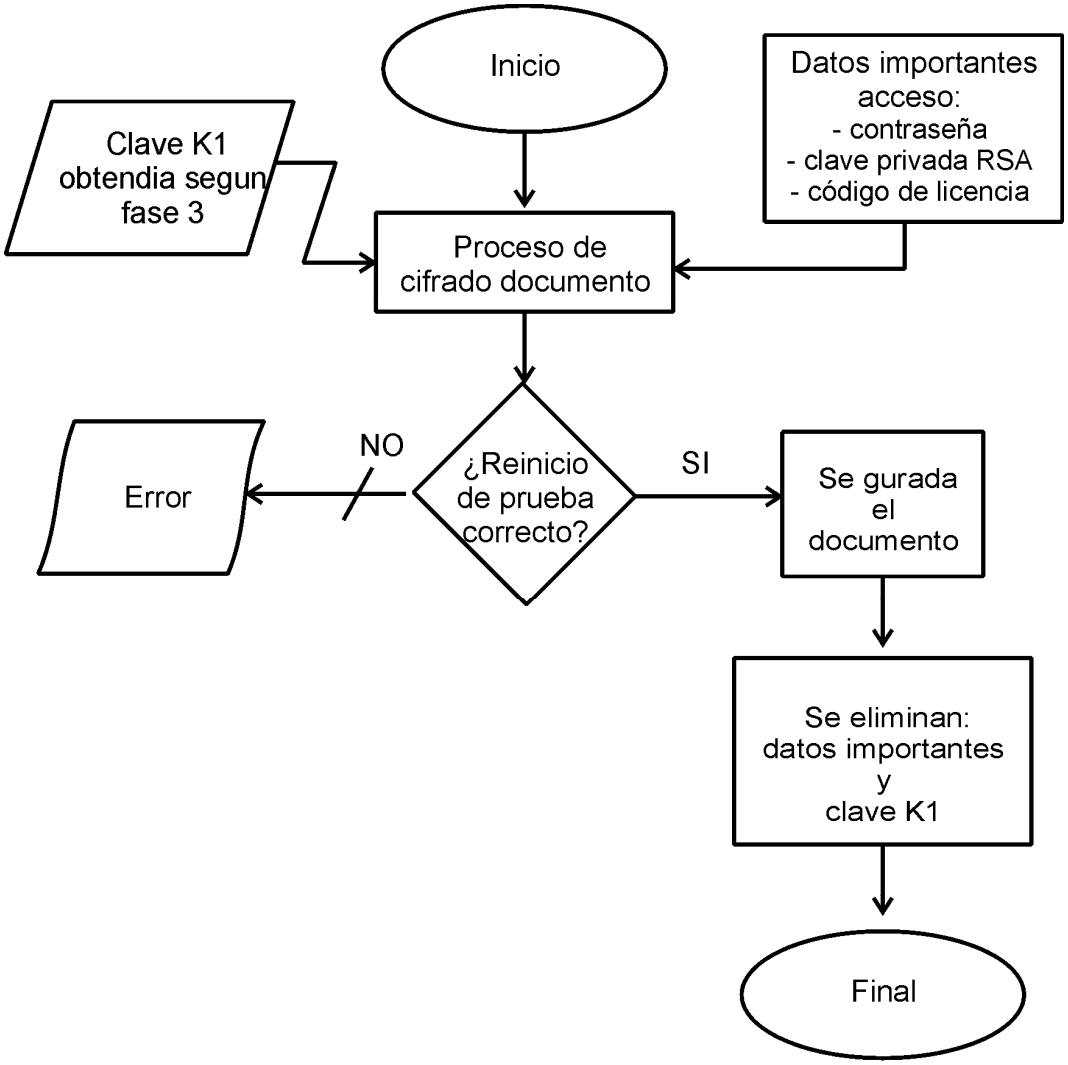
Inicio
Datos importantes acceso:
- contraseña
- clave privada RSA
- código de licencia
Clave K1 obtendia segun fase 3
Proceso de cifrado documento
¿Reinicio de prueba correcto?
NO
Error
SI
Se gurada el documento
Se eliminan: datos importantes y clave K1
Final

FIG. 4