(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 871 898**

(51) Int. CI.:

G06F 21/56 (2013.01)
H04L 29/06 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **26.10.2017 PCT/EP2017/077390**

(87) Fecha y número de publicación internacional: **03.05.2018 WO18077996**

(96) Fecha de presentación y número de la solicitud europea: **26.10.2017 E 17825369 (6)**

(97) Fecha y número de publicación de la concesión europea: **24.03.2021 EP 3516572**

(54) Título: **Indicador de reputación dinámica para optimizar operaciones de seguridad informática**

(30) Prioridad:

27.10.2016 US 201615336387

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
02.11.2021

(73) Titular/es:

BITDEFENDER IPR MANAGEMENT LTD. (100.0%)
Kreontos 12
1076 Nicosia, CY

(72) Inventor/es:

HAJMASAN, GHEORGHE-FLORIN;
MONDOC, ALEXANDRA y
PORTASE, RADU-MARIAN

(74) Agente/Representante:

ELZABURU, S.L.P

DESCRIPCIÓN

Indicador de reputación dinámica para optimizar operaciones de seguridad informática

Antecedentes

La invención se refiere a sistemas y métodos para proteger sistemas informáticos de software malicioso.

El software malicioso, también conocido como malware, afecta a una gran cantidad de sistemas informáticos en todo el mundo. En sus diversas formas, tales como virus informáticos, gusanos, rootkits ("encubridores") y software espía, el malware presenta un riesgo grave para millones de usuarios de ordenadores, haciéndolos vulnerables a la pérdida de datos e información confidencial, invasión de la privacidad, robo de identidad y pérdida de productividad. entre otros.

El software de seguridad se puede utilizar para detectar malware que infecta el sistema informático de un usuario, para eliminarlo y/o incapacitarlo. Se conocen en la técnica varias técnicas de detección de malware. Algunas se basan en contenido y se basan en hacer coincidir un fragmento de código del agente de malware con una biblioteca de firmas indicativas de malware. Otras técnicas convencionales, comúnmente conocidas como conductuales, detectan un conjunto de acciones sospechosas o indicativas de malware del agente de malware.

El software de seguridad puede representar una carga computacional significativa en el sistema informático de un usuario, lo que a menudo tiene un impacto medible en el rendimiento y la experiencia del usuario. La continua proliferación de software malicioso aumenta aún más la complejidad de las rutinas de detección de malware, así como el tamaño de las bases de datos de firmas. Para reducir los costos computacionales, el software de seguridad puede incorporar varios procedimientos de optimización. Los documentos de la bibliografía de patentes US2015/096018 A1 y US2007/240222 A1 constituyen una técnica anterior relevante relacionada con la presente invención.

Compendio

La presente invención está definida por las reivindicaciones independientes 1, 13 y 22 adjuntas. Según un aspecto, un sistema cliente comprende al menos un procesador de hardware configurado para ejecutar una entidad objetivo, un administrador de reputación y un motor anti-malware. El administrador de reputación se configura en respuesta a recibir un primer indicador de reputación de una entidad objetivo desde un servidor de reputación, el primer indicador de reputación indicativo de una probabilidad de que la entidad objetivo sea maliciosa, para transmitir el indicador de reputación al motor anti-malware. El administrador de reputación se configura, además, en respuesta a recibir el primer indicador de reputación, para determinar si la entidad objetivo ha realizado alguna de un conjunto de acciones predeterminadas durante un primer intervalo de tiempo. Cuando la entidad objetivo no ha realizado ninguna del conjunto de las acciones predeterminadas durante el primer intervalo de tiempo, el administrador de reputación determina un segundo indicador de reputación de la entidad objetivo, indicando el segundo indicador de reputación que es menos probable que la entidad objetivo sea maliciosa de lo indicado por el primer indicador de reputación. El administrador de reputación transmite además el segundo indicador de reputación al motor anti-malware y al servidor de reputación. Cuando la entidad objetivo ha realizado una primera acción del conjunto de acciones predeterminadas, el administrador de reputación determina un tercer indicador de reputación de la entidad objetivo, indicando el tercer indicador de reputación que es más probable que la entidad objetivo sea maliciosa de lo que indica el primer indicador de reputación. El administrador de reputación transmite además el tercer indicador de reputación al motor anti-malware y al servidor de reputación. El motor anti-malware está configurado, en respuesta a recibir el primer indicador de reputación, para emplear un primer protocolo para determinar si la entidad objetivo es maliciosa. El motor anti-malware se configura, además, en respuesta a recibir el segundo indicador de reputación, para emplear un segundo protocolo para determinar si la entidad objetivo es maliciosa, en donde el segundo protocolo es menos costoso computacionalmente que el primer protocolo. El motor anti-malware se configura, además, en respuesta a recibir el tercer indicador de reputación, para emplear un tercer protocolo para determinar si la entidad objetivo es maliciosa, en donde el tercer protocolo es más costoso computacionalmente que el primer protocolo.

Según otro aspecto, un sistema informático servidor comprende al menos un procesador de hardware configurado para realizar transacciones de administración de reputación con una pluralidad de sistemas cliente, en el que una transacción de administración de reputación comprende, en respuesta a una solicitud recibida de un sistema cliente de la pluralidad de sistemas cliente, recuperando un primer indicador de reputación de una entidad objetivo de una base de datos de reputación de la entidad, el primer indicador de reputación indicativo de una probabilidad de que la entidad objetivo sea maliciosa. La transacción comprende, además, en respuesta a la recuperación del primer indicador de reputación, transmitir el primer indicador de reputación al sistema del cliente y en respuesta a la transmisión del primer indicador de reputación, recibir un segundo indicador de reputación de la entidad objetivo desde el sistema del cliente. La transacción comprende, además, en respuesta a la recepción del segundo indicador de reputación, comparar el primer y el segundo indicadores de reputación. En respuesta, cuando el segundo indicador de reputación indica una probabilidad menor de que la entidad objetivo sea maliciosa que la indicada por el primer indicador de reputación, la transacción comprende además agregar el segundo indicador de reputación a una

colección de indicadores de reputación recibidos desde la pluralidad de sistemas cliente, en donde todos los miembros de la colección se determinan para instancias de la entidad de destino. La transacción comprende, además, en respuesta a agregar el segundo indicador de reputación a la colección, determinar si se cumple una condición de actualización de reputación y, en respuesta, cuando se cumple la condición de actualización, reemplazar el primer indicador de reputación en la base de datos de reputación con un indicador de reputación actualizado, determinado según la colección. La determinación del segundo indicador de reputación comprende emplear el sistema cliente, en respuesta a la recepción del primer indicador de reputación, para determinar si la entidad objetivo ha realizado alguna de un conjunto de acciones predeterminadas durante un primer intervalo de tiempo. Cuando la entidad objetivo no ha realizado ninguna del conjunto de acciones predeterminadas durante el primer intervalo de tiempo, la determinación del segundo indicador de reputación comprende además formular el segundo indicador de reputación para indicar que la entidad objetivo tiene menos probabilidades de ser maliciosa de lo que indica el primer indicador de reputación, y cuando la entidad objetivo ha realizado una primera acción del conjunto de acciones predeterminadas, formular el segundo indicador de reputación para indicar que es más probable que la entidad objetivo sea maliciosa de lo que indica el primer indicador de reputación.

Según otro aspecto, un medio legible por ordenador, no transitorio, almacena un conjunto de instrucciones que, cuando son ejecutadas por un procesador de hardware de un sistema cliente, hacen que el sistema cliente forme un administrador de reputación y un motor anti-malware. El sistema cliente ejecuta una entidad objetivo. El administrador de reputación se configura en respuesta a recibir un primer indicador de reputación de una entidad objetivo desde un servidor de reputación, siendo el primer indicador de reputación indicativo de una probabilidad de que la entidad objetivo sea maliciosa, para transmitir el indicador de reputación al motor anti-malware. El administrador de reputación se configura, además, en respuesta a recibir el primer indicador de reputación, para determinar si la entidad objetivo ha realizado alguna de un conjunto de acciones predeterminadas durante un primer intervalo de tiempo. Cuando la entidad objetivo no ha realizado ninguna del conjunto de las acciones predeterminadas durante el primer intervalo de tiempo, el administrador de reputación determina un segundo indicador de reputación de la entidad objetivo, indicando el segundo indicador de reputación que es menos probable que la entidad objetivo sea maliciosa. de lo indicado por el primer indicador de reputación. El administrador de reputación transmite además el segundo indicador de reputación al motor anti-malware y al servidor de reputación. Cuando la entidad objetivo ha realizado una primera acción del conjunto de acciones predeterminadas, el administrador de reputación determina un tercer indicador de reputación de la entidad objetivo, indicando el tercer indicador de reputación que es más probable que la entidad objetivo sea maliciosa de lo que indica el primer indicador de reputación. El administrador de reputación transmite además el tercer indicador de reputación al motor anti-malware y al servidor de reputación. El motor anti-malware está configurado, en respuesta a recibir el primer indicador de reputación, para emplear un primer protocolo para determinar si la entidad objetivo es maliciosa. El motor anti-malware se configura, además, en respuesta a recibir el segundo indicador de reputación, para emplear un segundo protocolo para determinar si la entidad objetivo es maliciosa, en donde el segundo protocolo es menos costoso computacionalmente que el primer protocolo. El motor anti-malware se configura, además, en respuesta a recibir el tercer indicador de reputación, para emplear un tercer protocolo para determinar si la entidad objetivo es maliciosa, en donde el tercer protocolo es más costoso computacionalmente que el primer protocolo.

Breve descripción de los dibujos

Los aspectos y ventajas anteriores de la presente invención se comprenderán mejor al leer la siguiente descripción detallada y al hacer referencia a los dibujos en los que:

La Figura **1** muestra un sistema anti-malware ejemplar que comprende una pluralidad de sistemas cliente y un servidor de reputación, según algunas realizaciones de la presente invención.

La Figura **2** muestra una vista detallada ejemplar de un entorno aislado tal como una intranet corporativa, protegida de amenazas a la seguridad informática de acuerdo con algunas realizaciones de la presente invención.

La Figura **3** muestra una entrada de base de datos de reputación ejemplar según algunas realizaciones de la presente invención.

La Figura **4-A** ilustra una configuración de hardware ejemplar de un sistema cliente según algunas realizaciones de la presente invención.

La Figura **4-B** muestra una configuración de hardware ejemplar de un servidor de reputación según algunas realizaciones de la presente invención.

La Figura **5** muestra un conjunto ejemplar de objetos de software que se ejecutan en un sistema cliente, que incluye una aplicación de seguridad configurada para proteger el sistema cliente de amenazas a la seguridad informática según algunas realizaciones de la presente invención.

La Figura **6** muestra componentes ejemplares de una aplicación de seguridad según algunas realizaciones de la presente invención.

La Figura **7** ilustra un intercambio de datos ejemplar entre un componente de administrador de reputación y un componente de motor anti-malware de la aplicación de seguridad, según algunas realizaciones de la presente invención.

La Figura **8** ilustra un intercambio de datos ejemplar entre un sistema cliente y un servidor de reputación según algunas realizaciones de la presente invención.

La Figura **9** muestra componentes ejemplares de una huella digital de una entidad ejecutable según algunas realizaciones de la presente invención.

La Figura **10** ilustra conjuntos y superconjuntos ejemplares de entidades ejecutables según algunas realizaciones de la presente invención.

La Figura **11** muestra una estructura de datos ejemplar asociada a una entidad ejecutable que se ejecuta en un sistema cliente, según algunas realizaciones de la presente invención.

La Figura **12-A** muestra una secuencia ejemplar de etapas realizadas por el componente de administrador de reputación de la aplicación de seguridad según algunas realizaciones de la presente invención.

La Figura **12-B** muestra una continuación de la secuencia ejemplar de etapas de la Figura **11-A** según algunas realizaciones de la presente invención.

La Figura **12-C** muestra otra continuación de la secuencia ejemplar de etapas de la Figura **11-A** según algunas realizaciones de la presente invención.

La Figura **12-D** muestra otra continuación más de la secuencia ejemplar de etapas de la Figura **11-A** según algunas realizaciones de la presente invención.

La Figura **13** ilustra una evolución temporal ejemplar de un indicador de reputación según algunas realizaciones de la presente invención.

La Figura **14** muestra una secuencia ejemplar de etapas realizadas por el componente de motor anti-malware de la aplicación de seguridad según algunas realizaciones de la presente invención.

La Figura **15** muestra una secuencia ejemplar de etapas realizadas por un servidor de reputación según algunas realizaciones de la presente invención.

Descripción detallada de realizaciones preferidas

En la siguiente descripción, se entiende que todas las conexiones citadas entre estructuras pueden ser conexiones operativas directas o conexiones operativas indirectas a través de estructuras intermedias. Un conjunto de elementos incluye uno o más elementos. Se entiende que cualquier citación de un elemento se refiere a al menos un elemento. Una pluralidad de elementos incluye al menos dos elementos. A menos que se requiera lo contrario, cualquier etapa del método descrito no necesita realizarse necesariamente en un orden ilustrado particular. Un primer elemento (por ejemplo, datos) derivado de un segundo elemento abarca un primer elemento igual al segundo elemento, así como un primer elemento generado procesando el segundo elemento y opcionalmente otros datos. Tomar una determinación o decisión según un parámetro engloba tomar la determinación o decisión según el parámetro y opcionalmente según otros datos. A menos que se especifique lo contrario, un indicador de alguna cantidad/datos puede ser la propia cantidad/datos, o un indicador diferente de la propia cantidad/datos. La seguridad informática abarca la protección de los usuarios y el equipo contra el acceso no intencionado o no autorizado a datos y/o hardware, contra la modificación no intencionada o no autorizada de datos y/o hardware, y contra la destrucción de datos y/o hardware. Un programa informático es una secuencia de instrucciones del procesador que lleva a cabo una tarea. Los programas informáticos descritos en algunas realizaciones de la presente invención pueden ser entidades o subentidades de software independientes (por ejemplo, subrutinas, bibliotecas) de otros programas informáticos. A menos que se especifique lo contrario, un proceso representa una instancia de un programa informático, que tiene un espacio de memoria separado y al menos un hilo de ejecución, almacenando el espacio de memoria una codificación de un conjunto de instrucciones de procesador (por ejemplo, código de máquina). A menos que se especifique lo contrario, un hash es una salida de una función hash. A menos que se especifique lo contrario, una función hash es una transformación matemática que asigna una secuencia de símbolos de longitud variable (por ejemplo, caracteres, bits) a una cadena de bits de longitud fija. Los medios legibles por ordenador abarcan medios no transitorios, tales como medios de almacenamiento magnéticos, ópticos y de semiconductores (por ejemplo, discos duros, discos ópticos, memoria flash, DRAM), así como enlaces de comunicaciones tales como cables conductores y enlaces de fibra óptica. Según algunas realizaciones, la presente invención proporciona, *entre otros,* sistemas informáticos que comprenden hardware (por ejemplo, uno o más procesadores) programados para realizar los métodos descritos en la presente memoria, así como instrucciones de codificación de medios legibles por ordenador para realizar los métodos descritos en este documento.

La siguiente descripción ilustra realizaciones de la invención a modo de ejemplo y no necesariamente a modo de limitación.

La Figura **1** muestra un sistema **5** de seguridad informático ejemplar según algunas realizaciones de la presente invención. El sistema **5** comprende un conjunto de sistemas cliente **10a-c** y un servidor central **14a** de reputación, conectado a través de una red **20** de comunicación**.** El servidor central **14a** de reputación, además, puede estar acoplado comunicativamente a una base de datos central **16a** de reputación**.** La red **20** puede ser una red de área amplia tal como Internet, mientras que partes de la red **20** también puede incluir una red de área local (LAN).

El sistema **5** puede comprender además un conjunto de entornos aislados **12a-b** conectado a la red **20.** Un entorno aislado puede representar, por ejemplo, la intranet de una empresa. Entornos 12a**-b** pueden estar separados del resto de la red **20** mediante cortafuegos y/u otros medios de defensa perimetral. La Figura **2** ilustra un entorno aislado **12** de este tipo**,** que comprende un conjunto de sistemas cliente **10d-e** y un servidor local **14b** de reputación, todos conectados a una red local **120.** La red **120** puede representar, por ejemplo, una red de área local. En algunas realizaciones, el entorno aislado **12** puede comprender además una base de datos local **16b** de reputación específica del entorno**,** acoplado comunicativamente al servidor local **14b** de reputación**.**

Los sistemas cliente **10a-e** representan sistemas informáticos de usuario final protegidos contra amenazas a la seguridad informática según algunas realizaciones de la presente invención. Los sistemas cliente **10a-e** ejemplares incluyen ordenadores personales, dispositivos informáticos y/o de telecomunicaciones como tabletas, teléfonos móviles, asistentes digitales personales (PDA), dispositivos informáticos portátiles (por ejemplo, relojes inteligentes), dispositivos domésticos como televisores o reproductores de música, o cualquier otro dispositivo electrónico que tenga un procesador y una memoria. Los sistemas cliente **10a-e** puede representar a clientes individuales de una empresa de seguridad informática; varios sistemas cliente pueden pertenecer al mismo cliente.

Los sistemas cliente **10a-e** pueden utilizar datos de reputación para aumentar la eficiencia de las operaciones de seguridad informática. En algunas formas de realización, los servidores **14a-b** de reputación manejan los datos de reputación a petición de los sistemas cliente **10a-e,** por ejemplo, para almacenar y recuperar selectivamente datos de reputación hacia/desde bases de datos **16a-b** de reputación**,** y transmitir dichos datos a un sistema cliente solicitante. Los detalles de dichas transacciones se dan a continuación.

Bases de datos **16a-b** de reputación pueden configurarse para almacenar datos de reputación asociados con varias entidades ejecutables (aplicaciones, componentes de un sistema operativo, procesos, bibliotecas, scripts, etc.). Los datos de reputación pueden almacenarse como una pluralidad de entradas, correspondiendo cada entrada a una entidad ejecutable distinta. La Figura **3** muestra una entrada **17** de base de datos de reputación ejemplar**,** que comprende un identificador de una entidad ejecutable (en este documento, denominada huella digital **70** de entidad) y un indicador **60** de reputación indicativo de una probabilidad de que la entidad respectiva sea maliciosa. Cada entrada de la base de datos de reputación puede comprender además una marca de tiempo (simbolizada como TS0) indicativa de un momento en el que el indicador **60** fue creado y/o un momento de la última actualización del indicador de reputación respectivo. La entrada **17** puede comprender además un indicador de vida útil de la reputación (RL) indicativo de la duración de la validez del indicador de reputación respectivo. Al especificar una vida útil limitada para los datos de reputación, algunas realizaciones fuerzan efectivamente una actualización periódica de dichos datos, conteniendo así la propagación de una posible infección con la entidad respectiva. El indicador de vida útil puede variar entre las entidades ejecutables; las reputaciones de algunas entidades que han demostrado ser maliciosas o benignas puede tener una vida útil ilimitada. Las huellas digitales de la entidad y los indicadores de reputación se describen con más detalle a continuación.

Algunas realizaciones distinguen entre la reputación actual de una entidad y la reputación histórica (HR) de la entidad respectiva. La reputación actual se refiere a la reputación de una entidad que actualmente reside o se ejecuta en un sistema cliente. La reputación histórica se usa aquí para denotar un valor de un indicador de reputación previamente calculado para otra instancia de la entidad ejecutable respectiva y almacenado en bases de datos **16a** y/o **16b.** Las reputaciones históricas pueden comprender datos de reputación agregados de otros sistemas de clientes y/o calculados en otras ocasiones en el pasado. Las reputaciones históricas pueden incluir una reputación determinada para la entidad respectiva por un analista de seguridad humana. A tales reputaciones históricas se les puede dar más peso en un proceso de decisión que a las reputaciones determinadas automáticamente, ya que es probable que sean más precisas que estas últimas.

El sistema de administración de reputación ejemplar ilustrado en las Figs. **1-2** está organizado de forma jerárquica. Para minimizar la latencia y mejorar la experiencia del usuario, los sistemas cliente **10a-e** primero puede buscar datos de reputación en la base de datos local **16b** de reputación**,** y luego, si es necesario, puede solicitar dichos datos de la base de datos central **16a** de reputación**.** En algunas realizaciones, la base de datos local **16b,** por lo tanto, puede considerarse como un caché local de base de datos central **16a.** Agregando datos de reputación de múltiples sistemas de clientes **10a-e,** la base de datos central **16a** de reputación puede adquirir rápidamente información sobre nuevas amenazas y distribuirla a otros sistemas cliente.

Configuraciones como se ilustran en la Figura **2** pueden permitir una manera específica del entorno de manejar los datos de reputación. En algunas realizaciones, la base de datos local **16b** de reputación almacena indicadores de

reputación diseñados específicamente para el entorno aislado respectivo. En uno de esos ejemplos, los sistemas cliente **10d-e** de una intranet corporativa ejecutan una aplicación de software X ampliamente utilizada, tal como Microsoft Office®. La aplicación X carga un módulo ejecutable Y, que es vulnerable al malware siempre que el sistema cliente respectivo esté conectado a Internet. Cuando los sistemas cliente **10d-e** no están conectados a Internet (por ejemplo, cuando el entorno **12** está protegido por medios de defensa perimetral), la aplicación X ya no sufre las vulnerabilidades asociadas a la conectividad a Internet. Por lo tanto, es posible que no sea necesario monitorear la aplicación X para detectar tales vulnerabilidades en los sistemas. **10d-e** (es decir, dentro de un entorno aislado **12),** mientras que dicho monitoreo puede ser importante en sistemas conectados directamente a Internet. De manera equivalente, la aplicación X puede tener una mayor confiabilidad dentro del entorno **12,** en comparación con el exterior del medio ambiente **12.**

En otro ejemplo de especificidad del entorno, una empresa utiliza una aplicación X de software de propietario, que normalmente no se encuentra fuera del entorno aislado **12.** Por lo tanto, es poco probable que otros sistemas cliente utilicen los datos de reputación asociados con la aplicación X. En algunas realizaciones, dichos datos de reputación solo se guardan en una base de datos **16b** de reputación específica del entorno**.,** y no en la base de datos central **16a** de reputación**.** Dichas configuraciones pueden aumentar la eficiencia de las búsquedas en la base de datos para los clientes que operan fuera de un entorno aislado **12,** así como para clientes que operan dentro del entorno **12.**

La Figura **4-A** muestra una configuración de hardware ejemplar de un sistema cliente **10** tal como los sistemas cliente **10a-e** de las Figs. **1-2,** según algunas realizaciones de la presente invención. El sistema cliente **10** puede representar un dispositivo informático corporativo, tal como un servidor empresarial, o un dispositivo de usuario final, tal como un ordenador personal o un teléfono inteligente, entre otros. La Figura **4-A** muestra un sistema informático con fines ilustrativos; otros sistemas cliente, tales como teléfonos móviles o dispositivos portátiles, pueden tener una configuración diferente. El sistema cliente **10** comprende un procesador **32,** una unidad **34** de memoria**,** un conjunto **36** de dispositivos de entrada**,** un conjunto **38** de dispositivos de salida**,** un conjunto **40** de dispositivos de almacenamiento**,** y un conjunto **42** de adaptadores de red**,** todo conectado por un concentrador **44** de controlador**.**

El procesador **32** comprende un dispositivo físico (por ejemplo, microprocesador, circuito integrado de múltiples núcleos formado en un sustrato semiconductor) configurado para ejecutar operaciones computacionales y/o lógicas con un conjunto de señales y/o datos. En algunas realizaciones, tales operaciones lógicas se entregan al procesador **32** en forma de una secuencia de instrucciones del procesador (por ejemplo, código de máquina u otro tipo de software). La unidad **34** de memoria puede comprender medios legibles por ordenador no transitorios (por ejemplo, RAM) que almacenan datos/señales a los que se accede o genera por el procesador **32** en el curso de la realización de instrucciones. Los dispositivos **36** de entrada pueden incluir teclados de ordenador, ratones y micrófonos, entre otros, incluidas las respectivas interfaces de hardware y/o adaptadores que permiten al usuario introducir datos y/o instrucciones en el sistema cliente **10.** Los dispositivos de salida **38** puede incluir pantallas de visualización y altavoces, entre otros, así como interfaces/adaptadores de hardware tales como tarjetas gráficas, lo que permite que el sistema **10** comunique datos a un usuario. En algunas realizaciones, los dispositivos **36** de entrada y los dispositivos **38** de salida pueden compartir una pieza común de hardware, como en el caso de los dispositivos de pantalla táctil. Los dispositivos **40** de almacenamiento incluyen medios legibles por ordenador que permiten el almacenamiento, lectura y escritura no transitorios de instrucciones y/o datos de software. Los dispositivos **40** de almacenamiento ejemplares incluyen discos ópticos y magnéticos y dispositivos de memoria flash, así como medios extraíbles como unidades y discos CD y/o DVD. El conjunto de adaptadores **42** de red habilita el sistema cliente **10** para conectarse a redes **20, 120,** y/o a otros dispositivos/sistemas informáticos. El concentrador **44** del controlador representa genéricamente la pluralidad de buses de sistema, periféricos y de conjuntos de chips, y/o todos los demás circuitos que permiten la intercomunicación de los dispositivos de hardware ilustrados. Por ejemplo, el concentrador **44** puede comprender el procesador **32** de conexión northbridge a la memoria **34,** y/o el procesador **32** de conexión southbridge a los dispositivos **36-38-40-42,** entre otros.

La **Figura 4-B** muestra una configuración de hardware ejemplar de un servidor **14** de reputación**,** que puede representar el servidor central **14a** de reputación en la Figura **1** o el servidor local **14b** de reputación en la Figura **2.** El servidor **14** comprende un procesador **132** de servidor**,** una memoria **134** de servidor, un conjunto de dispositivos **140** de almacenamiento del servidor**,** y un conjunto de adaptadores **142** de red, todo conectado por un concentrador **144** de controlador de servidor**.** El funcionamiento de los dispositivos **132, 134, 140,** y **142** puede reflejar el de los dispositivos **32, 34, 40,** y **42** descrito arriba. Por ejemplo, el procesador **132** de servidor puede comprender un circuito integrado configurado para ejecutar operaciones computacionales y/o lógicas con un conjunto de señales y/o datos. La memoria **134** del servidor puede comprender medios legibles por ordenador no transitorios (por ejemplo, RAM) que almacenan datos/señales a los que se accede o se generan por el procesador **132** en el curso de la ejecución de cálculos. Los adaptadores **142** de red habilitan al servidor **14** para conectarse a una red informática tal como las redes **20, 120.** En algunas realizaciones, el servidor **14** de reputación consiste en un componente de software que se ejecuta en un sistema cliente, como se muestra a continuación.

La Figura **5** muestra un conjunto ejemplar de objetos de software que se ejecutan en el sistema cliente **10** según algunas realizaciones de la presente invención. Un sistema operativo invitado (SO) **46** comprende software que proporciona una interfaz al hardware del sistema cliente **10,** y actúa como anfitrión para un conjunto de aplicaciones **52a-c** y **54** de software**.** El SO **46** puede incluir cualquier sistema operativo ampliamente disponible, tal como Windows®, MacOS®, Linux®, iOS® o Android™, entre otros. Las aplicaciones **52a-c** representan genéricamente

cualquier aplicación de usuario, tales como procesamiento de textos, procesamiento de imágenes, base de datos, navegador y aplicaciones de comunicación electrónica, entre otras. En algunas realizaciones, una aplicación **54** de seguridad está configurada para realizar operaciones anti-malware y/u otras operaciones como se detalla a continuación, con el fin de proteger el sistema cliente **10** de las amenazas a la seguridad informática. La aplicación **54** de seguridad puede ser un programa independiente o puede formar parte de un paquete de software. La aplicación **54** de seguridad puede ejecutarse, al menos en parte, a un nivel de kernel de privilegios de procesador.

En una realización alternativa a la ilustrada en la Figura **5,** el sistema operativo 46 y las aplicaciones **52a-**c pueden ejecutarse dentro de una máquina virtual (VM) expuesta por un hipervisor que se ejecuta en el sistema cliente **10.** Tales realizaciones pueden ser adecuadas para proteger arquitecturas basadas en la nube, tales como granjas de servidores y sistemas de infraestructura como servicio (IAAS), entre otros. Una máquina virtual se conoce comúnmente en la técnica como una abstracción (por ejemplo, emulación de software) de un sistema informático físico, comprendiendo la VM un procesador virtual, almacenamiento virtual, etc. En tales realizaciones, la aplicación **54** de seguridad puede ejecutarse dentro o fuera de la respectiva VM. Cuando se ejecuta en el exterior, la aplicación **54** de seguridad puede ejecutarse en el nivel de privilegio del procesador del hipervisor, o dentro de una máquina virtual separada. Una sola aplicación de seguridad puede proteger una pluralidad de VM que se ejecutan en el sistema cliente respectivo.

La Figura **6** muestra componentes ejemplares de la aplicación **54** de seguridad según algunas realizaciones de la presente invención. La aplicación 54 comprende un motor **56** anti-malware acoplado comunicativamente a un administrador **58** de reputación**.** El motor **56** anti-malware está configurado para determinar si el sistema cliente **10** comprende software malintencionado. En algunas realizaciones, el motor **56** puede eliminar aún más o incapacitar el malware de otro modo. Para realizar la detección de malware, el motor **56** puede emplear cualquier método conocido en la técnica. Los métodos anti-malware generalmente se dividen en dos categorías generales: basados en contenido y conductuales. Los métodos basados en contenido generalmente escanean el código de una entidad de software en busca de patrones indicativos de malware, comúnmente conocidos como firmas. Los métodos conductuales generalmente monitorean una entidad ejecutora para detectar ciertas acciones indicativas de malware realizadas por la entidad respectiva. Una entidad de software se considera maliciosa si está configurada para realizar cualquiera de un conjunto de operaciones maliciosas, por ejemplo, operaciones que conducen a una pérdida de privacidad, una pérdida de datos personales o sensibles o una pérdida de productividad por parte de un usuario. Algunos ejemplos incluyen modificar, borrar o cifrar datos sin el conocimiento o autorización de un usuario y alterar la ejecución de programas legítimos que se ejecutan en el sistema cliente **10.** Otros ejemplos de operaciones maliciosas incluyen la extracción de datos personales o sensibles de un usuario, tales como contraseñas, detalles de inicio de sesión, datos de tarjetas de crédito o cuentas bancarias o documentos confidenciales, entre otros. Otros ejemplos de acciones malintencionadas incluyen una interceptación no autorizada o la escucha clandestina de las conversaciones de un usuario y/o el intercambio de datos con terceros. Otros ejemplos incluyen el empleo del sistema cliente **10** para enviar comunicaciones no solicitadas (spam, anuncios) y utilizar el sistema cliente **10** para enviar solicitudes de datos maliciosos a un sistema informático remoto, como en un ataque de denegación de servicio.

En algunas realizaciones, el motor **56** monitorea y/o analiza un conjunto de entidades ejecutables que residen y/o están en ejecución en el sistema cliente **10.** Las entidades ejecutables ejemplares incluyen aplicaciones, procesos y módulos ejecutables, entre otros. Un módulo ejecutable es un componente o un bloque de construcción de un proceso, comprendiendo el componente respectivo código ejecutable. Los módulos ejecutables se pueden cargar y/o descargar a/desde la memoria durante el lanzamiento y/o ejecución del proceso respectivo. Los módulos ejecutables ejemplares incluyen un ejecutable principal de un proceso (tal como un archivo EXE en Windows®) y una biblioteca compartida (tal como una biblioteca vinculada dinámicamente, DLL), entre otros. En algunas realizaciones, el módulo ejecutable principal de un proceso comprende la primera instrucción de máquina ejecutada cuando se lanza el proceso respectivo. Las bibliotecas son secciones autónomas de código que implementan varios aspectos funcionales de un programa. Las bibliotecas compartidas pueden ser utilizadas de forma independiente por más de un programa. Otros ejemplos de entidades ejecutables incluyen, entre otros, scripts ejecutables llamados por el proceso respectivo (por ejemplo, Scripts de Perl, Visual Basic®, JavaScript® y Python), archivos interpretados (por ejemplo, Archivos JAR de Java®) y fragmentos de código inyectados en el respectivo proceso por otras entidades. La inyección de código es un término genérico utilizado en la técnica para indicar una familia de métodos para introducir una secuencia de código en el espacio de memoria de otra entidad para alterar la funcionalidad original de la entidad respectiva. Una persona experta en la técnica apreciará que los sistemas y métodos descritos aquí pueden traducirse a otros tipos de módulos ejecutables.

En algunas realizaciones, el administrador **58** de reputación está configurado para determinar los datos de reputación para una variedad de entidades ejecutables (objetos de software), incluidas aplicaciones, procesos y bibliotecas, para almacenar y/o recuperar dichos datos a/desde bases de datos de reputación, y para transmitir dichos datos al motor **56** anti-malware. En algunas realizaciones, el administrador **58** de reputación comprende un administrador **62** de la entidad, un monitor **64** de actividad, una calculadora **66** de huellas digitales**,** y un programador **68** de actualizaciones de reputación**.** El funcionamiento de estos componentes se describirá con más detalle a continuación. En una realización alternativa a la ilustrada en la Figura **6,** el administrador **62** de la entidad y el monitor **64** de actividad pueden ser parte del motor **56** anti-malware**.**

En algunas realizaciones, una base de datos **16c** de reputación del cliente comunicativamente acoplada al administrador **58** de reputación está configurada para almacenar temporalmente datos de reputación en medios legibles por ordenador del sistema cliente respectivo. Un servidor **14c** de reputación de cliente comprende un programa informático que se ejecuta en el sistema cliente **10,** estando el servidor **14c** configurado para agregar y/o recuperar selectivamente datos de reputación a la base de datos **16c** de reputación del cliente**.** La base de datos **16c** forma parte de la jerarquía de la base de datos descrita anteriormente y puede funcionar, al menos en parte, como un caché de bases de datos de reputación **16a-b** locales y/o centrales. En la configuración ejemplar mostrada en la Figura **6,** el administrador **58** de reputación emplea a un administrador **69** de comunicación para intercambiar datos con servidores remotos **14a-b.**

La Figura **7** muestra un intercambio de datos ejemplar entre administrador **58** y motor **56.** El administrador 58 de reputación coopera con el motor **56** anti-malware para aumentar la eficiencia de las operaciones anti-malware, por ejemplo, comunicando un indicador **60** de reputación asociado con una entidad de destino al motor **56.** En algunas formas de realización, el indicador **60** de reputación es indicativo de una probabilidad de que la entidad ejecutable respectiva sea maliciosa. Los indicadores **60** de reputación ejemplares incluyen una puntuación de reputación numérica que oscila desde un valor mínimo (por ejemplo, 0) a un valor máximo (por ejemplo, 100). En una realización ejemplar, una puntuación de reputación alta indica una alta probabilidad de que la entidad respectiva sea benigna (no maliciosa), mientras que las puntuaciones bajas indican una sospecha de malicia o una probabilidad de malicia desconocida/actualmente indeterminada. Otras realizaciones pueden usar una escala inversa en la que una puntuación baja indica un grado de confianza más alto que una puntuación alta. Los indicadores de reputación pueden variar continuamente entre el mínimo y el máximo, o pueden saltar entre un conjunto de mesetas discretas predeterminadas (por ejemplo, 10, 25, 50, 100). En otra realización, el indicador **60** de reputación puede tomar valores de una pluralidad de etiquetas, por ejemplo, "confiable", "moderadamente confiable", "no confiable" y "desconocido".

En respuesta al indicador **60** de reputación de recepción**,** algunas realizaciones del motor **56** anti-malware dan un trato preferencial a las entidades de confianza, en contraposición a las entidades desconocidas o que no son de confianza Por ejemplo, el motor **56** puede usar un protocolo de seguridad relajado para escanear/monitorear un objeto confiable y un protocolo de seguridad estricto para escanear/monitorear un objeto desconocido o no confiable, donde el protocolo de seguridad relajado es menos costoso computacionalmente que el protocolo de seguridad estricto. En uno de estos ejemplos, un protocolo de seguridad relajado puede instruir al motor **56** a emplear solo un subconjunto de métodos de detección de malware y/o solo un subconjunto de heurísticas de identificación de malware para escanear un objeto confiable, mientras que un protocolo de seguridad estricto puede usar un conjunto completo de métodos y/o heurísticas disponibles para el motor **56.** El costo computacional puede formularse generalmente de acuerdo con un recuento de ciclos de reloj del procesador y/o una memoria requerida para ejecutar un procedimiento particular. Por tanto, los procedimientos/protocolos que requieren más ciclos de reloj y/o más memoria pueden considerarse más costosos desde el punto de vista informático que los procedimientos/protocolos que requieren menos ciclos de reloj y/o menos memoria.

En algunas realizaciones, el indicador **60** de reputación varía en el tiempo, por ejemplo, en respuesta a diversas acciones realizadas por la entidad ejecutable respectiva. En un ejemplo en el que una alta reputación indica confianza, la reputación de una entidad objetivo aumenta con el tiempo, siempre que la entidad respectiva no realice ninguna acción indicativa de malware. La reputación respectiva también puede disminuir en respuesta a ciertas acciones de la entidad objetivo. En algunas realizaciones, la reputación de una entidad objetivo puede cambiar en respuesta a acciones de otras entidades relacionadas con la entidad objetivo-respectiva, por ejemplo, en respuesta a recibir una inyección de código procedente de otra entidad, en respuesta a una acción indicativa de malware realizada por una entidad secundaria de la entidad respectiva, etc. El administrador 58 de reputación puede recibir notificaciones de seguridad sobre diversas acciones de las entidades objetivo del motor **56** anti-malware, como se ilustra en la Figura **7.**

En algunas realizaciones, el administrador **58** de reputación busca el indicador de reputación de una entidad objetivo en una jerarquía de bases de datos de reputación. Para minimizar los retrasos en las comunicaciones y el tráfico de datos, el administrador **58** de reputación puede intentar primero recuperar datos de reputación de la base de datos **16c** del cliente. Cuando no puede encontrar datos coincidentes en la base de datos **16c** del cliente, el administrador 58 luego puede consultar la base de datos local **16b.** Luego, cuando aún no se encuentran los datos buscados, el administrador 58 puede proceder a solicitarlos desde una base de datos central **16a** de reputación central y remota**.** La Figura **8** ilustra los intercambios de datos entre el sistema cliente **10** y un servidor **14** de reputación remoto (que representa genéricamente a los servidores **14a-b-c** en las Figs. **1, 2,** y **6** respectivamente). En algunas realizaciones, dicha comunicación entre clientes y servidores de reputación remotos está cifrada para evitar ataques de intermediarios. El sistema cliente **10** puede transmitir una solicitud **71** de reputación al servidor **14,** indicando la solicitud 71 un identificador, tal como una huella digital de entidad de una entidad objetivo. En respuesta, el servidor **14** puede recuperar selectivamente el indicador **60** de reputación correspondiente a la entidad objetivo-respectiva de la base de datos **16** (que representa genéricamente bases de datos **16a** y/o **16b** en las Figs. **1** y **2,** respectivamente), y el indicador **60** de transmisión al sistema cliente **10.** El sistema cliente **10** también puede transmitir un informe **73** de reputación al servidor **14,** indicando el informe **73** un indicador de reputación actualizado destinado al almacenamiento en la base de datos **16.**

Para permitir una asociación inequívoca entre entidades ejecutables e indicadores de reputación, cada entidad ejecutable se identifica por medio de un token único llamado en la presente memoria huella digital de entidad. En algunas realizaciones, la calculadora **66** de huellas digitales está configurada para calcular dichas huellas digitales para entidades objetivo y módulos ejecutables. Las huellas digitales se pueden generar usando cualquier método conocido en la técnica, por ejemplo, mediante hash. El hash comprende aplicar una función hash a una parte de un objeto (por ejemplo, a una sección de código o al objeto completo) para obtener un número de tamaño fijo o una cadena de bits conocida como hash del objeto respectivo. Las funciones de hash ejemplares incluyen algoritmos de hash seguro (SHA) y de resumen de mensajes (MD).

En una realización preferida, una huella digital **70** de entidad se determina de acuerdo con un conjunto de huellas digitales de componentes individuales/bloques de construcción de la entidad respectiva. En el ejemplo que se muestra en la Figura **9,** una entidad ejecutable **80** comprende un conjunto de módulos ejecutables **82a-c.** Por ejemplo, en un entorno Windows®, los módulos **82a-c** puede comprender un ejecutable principal y dos DLL, respectivamente. En otros ejemplos de realización, los módulos **82a-c** puede representar otros componentes de la entidad (por ejemplo, scripts, archivos JAR, fragmentos de código inyectados, etc.). Una persona experta en la técnica apreciará que los sistemas y métodos descritos aquí pueden traducirse a otros tipos de bloques de construcción y otros niveles de granularidad.

En algunas realizaciones, una huella digital **74a-c** del módulo (por ejemplo, un hash) se calcula para cada uno de los componentes de la entidad ejecutable **80.** La calculadora **66** de huellas digitales luego puede determinar la huella digital **70** de la entidad como una combinación de huellas digitales **74a-c,** de módulos, por ejemplo, organizando las huellas digitales **74a-c** del módulo como una lista ordenada y/o concatenando las huellas digitales **74a-c** del módulo. Para facilitar la comparación y búsqueda de huellas digitales, algunas realizaciones pueden aplicar una segunda función hash a la concatenación/lista de huellas digitales **74a-c** del módulo. En algunas realizaciones, la huella digital **70** de la entidad además comprende una lista de indicadores de ruta, indicando cada indicador de ruta una ruta o ubicación de un componente/módulo correspondiente. Cuando el componente respectivo es un fragmento de código inyectado, la huella digital **70** de la entidad puede codificar una dirección de memoria y/o un tamaño del fragmento respectivo.

Cada huella digital **70** de entidad configurada como anteriormente representa de forma única una composición o disposición particular de componentes/bloques de construcción, en lugar de la propia entidad ejecutable como se ve, por ejemplo, por el sistema operativo 46. Por lo general, el sistema operativo asigna a cada entidad ejecutable un identificador único (por ejemplo, un ID de proceso), que permanece sin cambios durante toda la vida de la entidad respectiva, incluso en los casos en que la composición de la entidad respectiva cambia durante la vida de la entidad. Por el contrario, en algunas realizaciones de la presente invención, cuando la composición de una entidad ejecutable cambia (por ejemplo, cuando un proceso carga y descarga bibliotecas dinámicamente), la huella digital **70** de la entidad y, por lo tanto, la identidad de la entidad respectiva puede cambiar en consecuencia. Dicho de otra manera, en algunas realizaciones, cuando cambia la composición de una entidad, la entidad original deja de existir y se crea una nueva entidad. Dado que algunas realizaciones asocian de forma única un indicador de reputación con cada huella digital de entidad, cuando cambia la composición de una entidad ejecutable, su reputación también puede cambiar.

Una combinación particular de componentes/bloques de construcción puede aparecer en múltiples entidades ejecutables, como se muestra en la Figura **10.** Una entidad Y que tiene todos los componentes de otra entidad X se dice en la presente memoria que es un miembro de un superconjunto de entidad de la entidad X. En el ejemplo de la Figura **9,** el conjunto 84a es una entidad superconjunto de entidad **80a,** mientras el conjunto 84**b** es un superconjunto de entidades de ambas entidades **80a** y **80b .** En contraste, la entidad **80d** no es miembro de una entidad superconjunto de ninguna entidad **80a-c,** ya que la entidad **80d** no contiene el módulo A.exe. En algunas realizaciones, la reputación de una entidad puede afectar a la reputación de los miembros de un superconjunto de entidades de la entidad respectiva y, a su vez, puede verse afectada por la reputación de dichos miembros, como se muestra en detalle a continuación. En el ejemplo de la Figura **9,** un cambio en la reputación de la entidad **80a** puede provocar cambios en la reputación de las entidades **80b-c.**

En algunas realizaciones, el administrador **62** de la entidad (Figura **6)** mantiene una estructura de datos denominada aquí tabla de reputación, que describe una pluralidad de entidades ejecutables que residen y/o se ejecutan en el sistema cliente **10,** así como un conjunto de relaciones entre dichas entidades. Una tabla de reputación ejemplar comprende una pluralidad de entradas, correspondiendo cada entrada a una entidad ejecutable. Una de esas entradas **86** en la tabla de reputación se ilustra en la Figura **11.** La entrada **86** comprende una huella digital **70** de entidad de la entidad respectiva y un ID de entidad (EID) asignado a la entidad ejecutable respectiva por el sistema operativo **46.** Cuando la entidad respectiva es un proceso, un EID ejemplar comprende el ID de proceso - PID en Windows®. Tal configuración puede ser deseable porque permite una asociación inmediata entre huellas digitales **70** y el EID. Dado que la composición de una entidad puede cambiar con el tiempo (por ejemplo, al cargar dinámicamente una biblioteca), puede haber varias entradas en la tabla de reputación que tengan el mismo EID, pero huellas digitales distintas. Además, puede haber varias instancias de la misma entidad ejecutándose simultáneamente en el sistema cliente. **10,** por tanto, puede haber varias entradas en la tabla de reputación que tengan la misma huella digital pero distintos EID. En principio, cada uno de estos objetos puede tener su propio comportamiento y reputación y, por lo tanto, puede ser monitoreado/analizado de manera distinta a otros objetos.

En algunas realizaciones, la entrada **86** puede almacenar además un indicador de filiación de la entidad respectiva, por ejemplo, un identificador de una entidad principal de la entidad respectiva (ID principal - PID) y/o un identificador de una entidad secundaria de la entidad respectiva. Las entidades secundarias ejemplares son procesos secundarios, por ejemplo, creados por una entidad principal a través de la función CreateProcess de Windows® OS, o mediante el mecanismo de bifurcación en Linux®. La entrada **68** también puede incluir un conjunto de identificadores de entidades ejecutables que han inyectado código en la entidad respectiva, y/o un conjunto de identificadores de entidades en las que la entidad respectiva ha inyectado código. Estos identificadores, que pueden ser huellas digitales de entidades, están representados por una ID de entidad inyectada: INJID.

La entrada **68** de la tabla de reputación puede incluir además un conjunto de identificadores de miembros de un superconjunto de entidades de la entidad actual (superconjunto ID de miembro - SMID). En algunas realizaciones, cada SMID puede consistir en una huella digital de entidad del respectivo miembro de superconjunto. En una realización alternativa, cada SMID puede comprender un puntero a la entrada de la tabla de reputación asociada con el miembro de superconjunto de la entidad respectiva. Asociar la huella digital **70** con un PID, SMID y/o INJID puede facilitar la propagación de información de reputación entre entidades principales y secundarias, entre entidades y miembros del superconjunto y entre entidades que participan en la inyección de código, como se muestra con más detalle a continuación.

La reputación actual de una entidad objetivo puede variar en el tiempo, según el comportamiento de la entidad respectiva y/o según el comportamiento de otras instancias de la entidad respectiva. En algunas realizaciones, cuando la entidad objetivo no lleva a cabo ninguna acción sospechosa o indicativa de malware, la reputación de la entidad respectiva puede aumentar con el tiempo, por ejemplo, de acuerdo con un programa predeterminado. El programador **68** de actualizaciones de reputación (Figura **6)** puede configurarse para programar actualizaciones de reputación para entidades objetivo, por ejemplo, determinando un momento en el tiempo en el que debe tener lugar la próxima actualización del indicador de reputación, y un incremento ΔR por el cual el indicador de reputación actual debe cambiar.

Los datos temporales se pueden almacenar (por ejemplo, como una marca de tiempo) en un conjunto de campos de entrada **86** de la tabla de reputación**;** véanse, por ejemplo, indicadores **88** de tiempo en la Figura **11.** Uno de dichos indicadores de tiempo puede indicar el momento de la última actualización del indicador de reputación correspondiente a la huella digital de la entidad respectiva. Otro indicador de tiempo puede indicar un momento para la próxima actualización programada del indicador de reputación respectivo. Una pluralidad de dichos tiempos de actualización de reputación puede, por tanto, hacer una crónica detallada de la dinámica de la reputación de cada entidad objetivo. Otro indicador de tiempo ejemplar puede indicar un tiempo de expiración de una reputación histórica de la entidad respectiva, por ejemplo, el momento en el que debe realizarse la siguiente búsqueda en la base de datos para la reputación histórica. La duración de la reputación histórica puede variar entre las entidades ejecutables. Al especificar una vida útil limitada para los datos de reputación de caché, algunas realizaciones fuerzan efectivamente una actualización de los datos de reputación de los servidores **14** de reputación locales o remotos**,** conteniendo así una infección potencial.

En algunas realizaciones, el monitor **64** de actividad (Figura **6)** está configurado para detectar la ocurrencia de eventos del ciclo de vida de entidades tales como aplicaciones y procesos que se ejecutan dentro del sistema cliente **10.** Los eventos ejemplares del ciclo de vida incluyen el lanzamiento y/o la terminación de una entidad ejecutable, la carga y/o descarga dinámica de bibliotecas por parte de la entidad respectiva, la generación de entidades secundarias y la inyección de código, entre otros.

El monitor **64** de actividad puede determinar además las relaciones entre objetos, como qué proceso cargó qué módulo ejecutable, qué entidad es principal o secundaria de qué entidad, qué entidad ha inyectado o recibido código inyectado de qué entidad, etc. En algunas realizaciones, el monitor **64** de actividad colabora con el administrador **62** de la entidad para completar la entrada **68** de la tabla de reputación de cada entidad con los datos requeridos (por ejemplo, EID, PID, SMID, INJID, etc.). Para realizar tareas tales como detectar el lanzamiento de una entidad y/o detectar la inyección de código, el monitor 64 puede emplear cualquier método conocido en la técnica, tal como llamar o conectar determinadas funciones del sistema operativo. Por ejemplo, en un sistema que ejecuta Windows® OS, el monitor 64 puede interceptar una llamada a una función LoadLibrary o a una función CreateFileMapping para detectar la carga de un módulo ejecutable. En otro ejemplo, el monitor **64** puede registrar una devolución de llamada PsSetCreateProcessNotifyRoutine para detectar el inicio de un nuevo proceso, y/o puede conectar la función CreateRemoteThread para detectar la ejecución del código inyectado.

La Figura **12-A** muestra una secuencia ejemplar de etapas realizadas por el administrador **58** de reputación en algunas realizaciones de la presente invención. Una secuencia de etapas **302-304** puede esperar una notificación. En algunas realizaciones, el administrador **58** de reputación es notificado por el monitor **64** de actividad sobre la ocurrencia de un evento del ciclo de vida de una entidad, tal como el lanzamiento de un proceso, la carga de una DLL, etc. El administrador **58** también puede ser notificado por el programador **68** de que una determinada entrada de la tabla de reputación debe actualizarse. El administrador 58 además puede recibir notificaciones del motor **56** anti-malware cuando una entidad objetivo realiza ciertas acciones que pueden ser relevantes para la seguridad informática (véase la Figura **7).** Cuando se recibe una notificación, la etapa **304** puede identificar una fuente y/o tipo de la notificación respectiva, y puede identificar además las entidades objetivo que causan la notificación respectiva

y/o las entidades que se ven afectadas por la notificación respectiva. En algunas realizaciones, el monitor **64** de la entidad puede determinar la identidad de dichas entidades a partir de las estructuras de datos utilizadas por el sistema operativo **46** para representar a cada entidad actualmente en ejecución. Por ejemplo, en Windows, cada proceso se representa como un bloque de proceso ejecutivo (EPROCESS), que comprende, entre otros, identificadores de cada uno de los hilos del proceso respectivo, y un ID de proceso único que permite al sistema operativo **46** identificar el proceso respectivo de una pluralidad de procesos en ejecución. Las representaciones de procesos similares están disponibles en Linux® y en otros sistemas operativos. Cuando más de una entidad se ve afectada por la notificación, la etapa **304** puede incluir además determinar una relación entre las respectivas entidades. Por ejemplo, cuando un proceso principal lanza un proceso secundario, el monitor **64** de entidad puede registrar la identidad del secundario y el principal, y el tipo de relación (filiación).

La Figura **12-B** muestra una secuencia ejemplar de etapas llevadas a cabo por el administrador **58** de reputación en respuesta a recibir una notificación procedente del monitor **64** de actividad**.** Tales notificaciones comunican típicamente la ocurrencia de un evento del ciclo de vida relacionado con una entidad objetivo. En una etapa **322,** la calculadora **66** de huellas digitales puede calcular una huella digital de entidad de la respectiva entidad objetivo. La etapa **322** puede comprender enumerar módulos/bloques de construcción de la entidad objetivo, identificar una sección de memoria que contiene cada módulo, calcular huellas digitales del módulo y ensamblar la huella digital de la entidad de acuerdo con las huellas digitales del módulo individual (véase la Figura **9** y descripción asociada). En una etapa **323,** el administrador **62** de la entidad puede buscar el ID de entidad (EID) de la entidad objetivo en la tabla de reputación, para determinar si un objeto con el mismo EID ya está siendo rastreado/analizado. El sistema operativo utiliza el ID de entidad para identificar la entidad objetivo; en un entorno Windows®, un EID ejemplar es el ID de proceso (PID) de un proceso actualmente en ejecución. Cuando el EID respectivo es nuevo (lo que indica que la entidad de destino es una nueva instancia de un objeto ejecutable), en una etapa **325,** el administrador **62** de la entidad puede crear una nueva entidad de tabla de reputación para representar la entidad objetivo. Cuando el EID respectivo no es nuevo (por ejemplo, cuando la composición del módulo de la entidad de destino está cambiando, por ejemplo, un proceso está cargando una biblioteca), una etapa **324** puede determinar si la tabla de reputación actualmente enumera una entidad con la misma huella digital **70** como entidad objetivo. Cuando la tabla de reputación ya contiene una entrada con la misma huella digital, el administrador **58** de reputación puede avanzar a una etapa **326** descrita más adelante. Tales situaciones pueden surgir, por ejemplo, cuando el evento del ciclo de vida detectado se refiere a una entidad objetivo que ya se está ejecutando. Cuando la huella digital de la entidad objetivo es nueva (no se incluye ninguna entidad con la misma huella digital en la tabla de reputación), el administrador **62** de la entidad puede crear una nueva entrada de tabla para la entidad objetivo-respectiva.

En algunas realizaciones, un cambio en la composición del módulo de una entidad provoca un cambio en la huella digital de la entidad. Por lo tanto, aunque la entidad respectiva no ha sido terminada, desde la perspectiva de las huellas digitales puede parecer que la entidad anterior ha dejado de existir y ha aparecido una nueva entidad en el sistema cliente **10.** En tales casos, así como en los casos en que se ha lanzado una nueva entidad, en una etapa **336** el administrador **58** de reputación puede intentar buscar datos históricos de reputación asociados con la huella digital de la entidad respectiva. La etapa **336** puede incluir, por ejemplo, el administrador **58** de reputación enviando solicitud **71** de reputación al servidor **14** de reputación (véase, por ejemplo, la Figura **8).** Cuando existen datos históricos de reputación para la huella digital respectiva, el servidor **14** puede recuperar selectivamente dichos datos de la base de datos **16** y transmitir el indicador 60 al sistema cliente **10.** Tal situación puede surgir cuando se ha observado antes una instancia de la entidad respectiva (combinación de módulos ejecutables), posiblemente ejecutándose en un sistema cliente distinto, y se ha calculado y almacenado una reputación de la entidad respectiva en la base de datos **16.** Al recibir el indicador **60** de reputación **,** en una etapa **338,** el administrador **58** de reputación puede establecer el indicador de reputación actual de la entidad objetivo a un valor determinado de acuerdo con la reputación histórica de la entidad respectiva. En una realización ejemplar, la reputación actual se establece para ser igual a la reputación histórica.

Cuando la etapa **337** determina que no hay reputación histórica disponible para la entidad objetivo, el administrador de reputación avanza a una etapa **339.** Esta situación puede surgir, por ejemplo, cuando aparece un nuevo software en el mercado (por ejemplo, un nuevo producto o una actualización de software), cuando una entrada de la base de datos para la entidad respectiva ha expirado o cuando el servidor **14** no está disponible (por ejemplo, falta de conexión a la red, servidor inactivo). En la etapa **339,** el administrador **64** de la entidad puede determinar si la entidad objetivo es una entidad secundaria de una entidad principal actualmente listada en la tabla de reputación. En caso afirmativo, en una etapa **340** algunas realizaciones establecen la reputación de la entidad objetivo en un valor determinado de acuerdo con la reputación de la entidad principal (por ejemplo, igual o menor que la reputación de la principal).

En una etapa **341,** el administrador **64** de la entidad puede determinar si hay miembros de un superconjunto de entidades de la entidad objetivo presente actualmente en la tabla de reputación. En caso afirmativo, algunas realizaciones del administrador **58** de reputación establecen la reputación actual de la entidad objetivo en un valor determinado de acuerdo con la reputación de la entidad miembro del superconjunto (por ejemplo, igual a la reputación del miembro del superconjunto). Un razonamiento que respalda tal elección de reputación considera que, dado que los miembros del superconjunto comprenden una mayoría sustancial (o todos) de los módulos ejecutables de la entidad objetivo, la reputación de la entidad objetivo puede deducirse de la reputación de un miembro del superconjunto.

Cuando no hay entidades principales o entidades miembro de superconjunto, en una etapa **344** el administrador **58** de reputación puede establecer la reputación actual de la entidad objetivo a un valor por defecto, predeterminado. Por ejemplo, la reputación de una entidad desconocida puede establecerse en un valor indicativo de un bajo grado de confianza (por ejemplo, no confiable, desconocido, R = 0). La reputación inicial también puede depender de un tipo de la entidad objetivo o de un conjunto de características de la entidad objetivo. Por ejemplo, una entidad descargada de Internet puede recibir un valor de reputación inicial R = 0 si no está firmada digitalmente, y un valor de reputación inicial R = 20% cuando está firmada.

En una etapa **326,** el programador **68** de actualizaciones puede programar una próxima actualización de la entrada de la tabla de reputación de la entidad objetivo. En algunas realizaciones, la reputación de una entidad objetivo varía con el tiempo. Por ejemplo, cuando la entidad respectiva no realiza ninguna acción considerada sospechosa o indicativa de malware, y/o cuando la entidad objetivo no comprende ningún patrón de código que coincida con una firma indicativa de malware, el indicador de reputación de la entidad respectiva puede progresar hacia valores que indican un mayor nivel de confianza (por ejemplo, R puede aumentar hacia el 100% de confianza). Un escenario de variación ejemplar para el indicador de reputación en una realización en el que valores de R más altos indica más confianza se muestra en la Figura **13.** El indicador de reputación ilustrado puede saltar entre un conjunto de valores predeterminados R_1, R_2, R_3, etc. Dichos cambios en la reputación pueden ocurrir en momentos predeterminados, por ejemplo, R puede aumentar desde el valor R_2 al valor R_3 en una instancia de tiempo t_2 (por ejemplo, medido con respecto al momento de creación de la entidad objetivo-respectiva).

El valor R puede determinarse según un tiempo transcurrido desde la creación/lanzamiento de la entidad objetivo-respectiva. En una realización alternativa, R puede aumentar después de que haya transcurrido un intervalo de tiempo Δt desde la ocurrencia de un evento anterior (por ejemplo, un aumento previo en la reputación, un evento de seguridad, etc.). En algunas realizaciones, los intervalos de tiempo Δt pueden variar por si mismos en el tiempo. Por ejemplo, los aumentos de reputación pueden ser menos frecuentes en la vida temprana de una entidad que en una etapa posterior. En otro ejemplo, la duración del intervalo de tiempo puede depender del valor actual de la reputación. Los incrementos de reputación pueden ser proporcional al valor de reputación actual (por ejemplo, cada vez, R puede aumentar en un 20%). Los incrementos de reputación ΔR también pueden variar con el tiempo. Por ejemplo, R puede aumentar en pequeñas cantidades en la vida temprana de una entidad y en cantidades mayores en momentos posteriores. Una razón fundamental que respalda esta dinámica de reputación es que el software malintencionado normalmente realiza su actividad en las primeras etapas de existencia (es decir, poco después del lanzamiento), por lo que cuando una entidad se comporta bien durante un tiempo suficiente, puede ser seguro asumir que no es malintencionado.

En algunas realizaciones, los intervalos de tiempo Δt y/o los incrementos de reputación ΔR pueden ser específicos del tipo de entidad, en el sentido de que pueden variar según un tipo de la entidad objetivo-respectiva. Por ejemplo, la dinámica de reputación de una entidad que está firmada digitalmente puede diferir de la dinámica de reputación de una entidad que no lo está. En otro ejemplo, la dinámica de reputación de una entidad puede diferir según si la entidad respectiva está configurada para acceder a Internet o no.

En algunas realizaciones, programar una actualización de reputación (etapa **326** en la Figura **12-B)** comprende determinar un intervalo de tiempo para la próxima actualización y/o un aumento de reputación. Una etapa **328** luego actualiza una entrada de la tabla de reputación de la entidad respectiva en consecuencia. Los cambios en la reputación actual de una entidad objetivo pueden desencadenar cambios en la reputación actual de otras entidades, por ejemplo, una entidad principal de la entidad objetivo o una entrada de un miembro de superconjunto de la entidad objetivo. Cuando es así, en una etapa **330,** el administrador **58** de reputación realiza dichas actualizaciones. En una secuencia de etapas **332-334,** el administrador **58** de reputación transmite el indicador **60** de reputación al motor **56** anti-malware y al servidor **14** de reputación**.**

La Figura **12-C** muestra una secuencia ejemplar de etapas ejecutadas por el administrador **58** de reputación en respuesta a una notificación procedente del programador **68** de actualizaciones (etiqueta B en la Figura **12-A)**. Una notificación de este tipo identifica típicamente una entidad objetivo e indica que el indicador de reputación de la entidad objetivo-respectiva debe actualizarse. En una etapa **356,** el administrador **58** de reputación puede actualizar el indicador de reputación de la entidad respectiva, por ejemplo, de acuerdo con un incremento de reputación almacenado en un campo de la entrada de la tabla de reputación de la entidad respectiva (véase, por ejemplo, la Figura **11).** En una etapa **358,** el programador **68** de actualización de reputación puede programar la próxima actualización de reputación, por ejemplo, determinando un intervalo de tiempo Δt y un incremento de reputación ΔR, y escribiendo estos valores en los campos correspondientes de la entrada de la tabla de reputación de la entidad objetivo-respectiva (etapa **360**). El incremento de reputación ΔR puede determinarse como un valor absoluto o como una fracción de la reputación actual (por ejemplo, 20%). Una secuencia de etapas **360-364** actualiza las entradas de la tabla de otras entidades relacionadas con la entidad objetivo y transmite el indicador **60** de reputación al motor **56** anti-malware**.**

En una etapa adicional **366,** el administrador **58** de reputación puede desencadenar una actualización de la base de datos **16** de reputación para reflejar el cambio de reputación de la entidad objetivo y posiblemente de otras entidades relacionadas. La etapa 366 puede incluir el envío de un informe **73** de reputación que comprende los indicadores de reputación actualizados al servidor **14** de reputación (por ejemplo, Figura **8).** Dicha actualización hace que las

nuevas reputaciones estén disponibles para otros sistemas cliente que ejecutan otras instancias con la misma entidad objetivo, propagando así el conocimiento de seguridad informática a través de la red de clientes. De una manera ejemplar en la que el servidor **14** de reputación maneja el informe **73,** véase a continuación en relación con la Figura **15.**

La Figura **12-D** muestra una secuencia ejemplar de etapas realizadas por el administrador **58** de reputación en respuesta a una notificación de seguridad del motor **56** anti-malware (véase, por ejemplo, la Figura **7).** Dichas notificaciones pueden generarse cuando el motor anti-malware determina que se sospecha que una entidad objetivo en particular es maliciosa. En algunas realizaciones, el motor **56** puede notificar al administrador **58** de reputación sobre la ocurrencia de un evento relevante para la seguridad, o de un evento que sea indicativo de malware. Los eventos ejemplares comprenden, entre otros, un intento de acceder a la memoria de una manera que viole un permiso de acceso a la memoria, un intento de ejecutar cierta función del sistema operativo (por ejemplo, crear un archivo de disco, editar una entrada de registro, etc.), un intentar de realizar ciertas operaciones (por ejemplo, inyectar código en otra entidad, descargar un archivo de un servidor remoto). La notificación **72** puede comprender un identificador de una entidad que ha causado o que se ha visto afectada por el evento respectivo, y un indicador de un tipo de evento respectivo. Otro ejemplo de notificación se puede generar en respuesta a un escáner de firmas que encuentra una firma de código malicioso mientras analiza el código de una entidad objetivo.

En respuesta a recibir una notificación de seguridad **72,** en una etapa **372** el administrador **58** de reputación puede determinar un nuevo valor para el indicador de reputación de la entidad objetivo-respectiva. En algunas realizaciones, cuando una entidad realiza una acción que es indicativa de malware o que hace que la entidad respectiva sea sospechosa de malicia, la reputación de la entidad respectiva cambia en la dirección de una menor confiabilidad. Este aspecto se ilustra en la Figura **13,** donde el valor de R cae en respuesta a un evento de seguridad. El administrador **58** de reputación puede determinar la magnitud de la caída de acuerdo con un conjunto de reglas/política de seguridad. La magnitud de la caída puede expresarse como un valor absoluto o como una fracción del valor de reputación actual (por ejemplo, 50%).

En algunas realizaciones, el tamaño de la caída en la reputación que se produce en tal ocasión varía según el tipo de evento o el tipo de notificación de seguridad. Algunos eventos/acciones son más claramente indicativos de malware y, por lo tanto, pueden provocar mayores caídas en la reputación. Otros eventos no son necesariamente indicativos de malicia, pero pueden serlo cuando ocurren junto con otros eventos o junto con ciertas acciones realizadas por la entidad objetivo. El cambio de reputación provocado por tales eventos o acciones puede ser relativamente menor que el asociado con un evento/acción claramente malicioso. Algunas notificaciones de seguridad pueden causar una pérdida total de reputación para la entidad objetivo-respectiva. En algunas realizaciones, la caída de reputación puede determinarse según si el indicador de reputación respectivo ha sufrido otras caídas en el pasado, según el tiempo transcurrido desde la caída anterior de reputación y/o según un tipo de notificación de seguridad que haya disparado la anterior caída de reputación. Algunos agentes de malware organizan acciones maliciosas en una pluralidad de entidades y distribuyen dichas acciones en el tiempo para evitar la detección. Condicionar una caída actual en la reputación a un historial previo de notificaciones de seguridad puede abordar algunos de dichos escenarios de malware sofisticados. En algunas realizaciones, el cambio de reputación que se produce en la etapa **372** se calcula de acuerdo con la reputación actual de la entidad objetivo y/o de acuerdo con la reputación actual de otras entidades. En uno de estos ejemplos, cuando una entidad X inyecta código en una entidad Y, la reputación de la más confiable de las dos entidades puede llegar a ser igual a la reputación actual de la menos confiable.

En una etapa **374,** el administrador **58** de reputación puede programar una actualización de la reputación de la entidad objetivo-respectiva, por ejemplo, generando un intervalo de tiempo Δt y un incremento de reputación ΔR. Una etapa **376** adicional puede guardar dichos datos en la entrada de la tabla de reputación de la entidad respectiva. En algunas realizaciones, los valores de Δt y/o ΔR pueden variar según un tipo de notificación de seguridad. En uno de esos ejemplos, cuando una entidad ha realizado una acción que es claramente indicativa de malicia, es posible que no se confíe en ella durante un período de tiempo relativamente largo. Por el contrario, después de una caída causada por un evento menos crítico para la seguridad, la reputación de una entidad objetivo puede volver a aumentar relativamente rápido.

En algunas realizaciones, una secuencia de etapas **376-380-382** puede actualizar las entradas de la tabla de reputación de otras entidades relacionadas con la entidad objetivo (si existe), puede transmitir el indicador **60** de reputación al motor **56** anti-malware**,** y puede informar cambios en la reputación al servidor **14.**

La Figura **14** muestra una secuencia ejemplar de etapas llevadas a cabo por el motor **56** anti-malware según algunas realizaciones de la presente invención. El motor **56** puede configurarse para llevar a cabo actividades de detección, prevención y/o limpieza de malware de acuerdo con las reputaciones específicas de la entidad (etapa **392).** Dicho de otra manera, el motor **56** anti-malware puede monitorear y/o analizar cada entidad ejecutable de acuerdo con un protocolo/política específica de la entidad, donde la política/protocolo respectivo puede variar de una entidad a otra de acuerdo con un indicador de reputación de cada entidad. En algunas realizaciones, las entidades que tienen una reputación que indica una alta confiabilidad pueden analizarse usando procedimientos menos costosos computacionalmente que las entidades que son menos confiables.

La detección de malware de comportamiento generalmente usa un conjunto de reglas para determinar si una entidad objetivo es maliciosa. A menudo, estas reglas se denominan heurísticas. Una heurística ejemplar puede decir, por ejemplo, que, si una primera entidad inyecta un fragmento de código en una segunda entidad, y el código respectivo intenta descargar un archivo de Internet, entonces la primera entidad probablemente sea maliciosa. Para implementar tales heurísticas, el motor **56** anti-malware puede necesitar monitorear una variedad de eventos (por ejemplo, inyección de código e intento de conectarse a un servicio remoto, en el ejemplo anterior). Algunos de estos eventos son más costosos desde el punto de vista computacional de monitorear que otros. Además, algunas heurísticas pueden ser intrínsecamente más complejas y/o más difíciles de aplicar que otras. Las heurísticas complejas pueden incluir una combinación de heurísticas más simples, por ejemplo "aplique el método A; si el resultado de A es X, aplique el método B; si el resultado de B es Y, verifique además la condición Z, etc."

Algunos ejemplos de heurísticas costosas incluyen la heurística utilizada para detectar ransomware (que comprende monitorear toda la actividad del sistema de archivos, cada lectura, escritura y/o copia de archivos) y heurísticas relacionadas con las claves de registro del sistema operativo (por ejemplo, que comprende interceptar cada escritura en el registro y determinar si comprende un intento de modificar una clave en particular). Otro ejemplo de una heurística costosa requiere detectar una llamada a una función del sistema operativo de uso frecuente (por ejemplo, CreateFile, ReadFile); la detección de tales llamadas puede dar como resultado una sobrecarga sustancial. Por el contrario, la detección de una llamada a una función del sistema operativo que se utiliza con mucha moderación en el funcionamiento normal (por ejemplo, CreateRemoteThread) puede suponer una carga mucho menor para el sistema cliente **10.**

En algunas realizaciones, la obtención de un protocolo de detección dependiente de la reputación comprende la monitorización de eventos variables y/o la complejidad de las heurísticas según un indicador de reputación. Dicho de otra manera, el motor **56** anti-malware puede monitorear una entidad confiable usando menos heurísticas y relativamente más simples que una entidad no confiable. El motor **56** también puede deshabilitar la detección de ciertos eventos o comportamientos al monitorear entidades confiables. Los métodos anti-malware basados en contenido también pueden ser específicos para la reputación, por ejemplo, ajustando el tamaño de una base de datos de firmas de acuerdo con la reputación. En uno de estos ejemplos, las entidades confiables pueden verificarse para detectar la presencia de un conjunto relativamente pequeño de firmas indicadoras de malware, mientras que las entidades no confiables pueden verificarse utilizando un conjunto de firmas sustancialmente mayor.

En la Tabla 1 se muestra un ejemplo de ajuste del protocolo de monitoreo con el indicador de reputación.

Tabla 1

Indicador de reputación	**Protocolo**
0% de confianza	Monitoreo máximo, emplee todas las heurísticas disponibles
10% de confianza	Deshabilite algunas heurísticas costosas
...	
80% de confianza	Monitorear la inyección de código y eliminar/copiar archivos
90% de confianza	Solo monitorear para inyección de código
100% de confianza	No monitorear en absoluto

Volviendo a la Figura **14,** en una secuencia de etapas **392-394,** motor **56** anti-malware está configurado para esperar la ocurrencia de un evento como se describe en un protocolo específico de reputación. Además de estos eventos relevantes para la seguridad, el motor **56** puede recibir indicadores de reputación del administrador **58** de reputación**.** Recibir un indicador de reputación puede indicar que la reputación de una entidad en particular ha cambiado. En respuesta a recibir un indicador de reputación (etapa **396),** en una etapa **398** el motor anti-malware puede identificar la entidad objetivo-respectiva y actualizar el protocolo/política de monitoreo que se aplica a la entidad respectiva de acuerdo con el valor recibido del indicador de reputación.

Cuando el evento detectado comprende un evento de seguridad (por ejemplo, una entidad ha inyectado código en otra entidad), en una etapa **402** el motor **56** anti-malware puede identificar una entidad objetivo que causó el evento respectivo y/o que fue afectada por el evento respectivo. Una etapa **404** adicional puede formular una notificación de seguridad de acuerdo con la identidad de la entidad objetivo y con el tipo de evento detectado, y transmitir la notificación de seguridad respectiva al administrador **58** de reputación.

La Figura **15** muestra una secuencia ejemplar de etapas llevadas a cabo por el servidor **14** de reputación (por ejemplo, servidores **14a-b** en las Figs. **1-2)** según algunas realizaciones de la presente invención. En una secuencia de etapas **412-414,** el servidor **14** puede escuchar la comunicación de los sistemas cliente **10.** Cuando se recibe una comunicación, una etapa **416** puede determinar si la comunicación respectiva es una solicitud de reputación (véase, por ejemplo, la Figura **8).** En caso afirmativo, servidor **14** puede buscar datos históricos de reputación asociados con

la huella digital de la entidad incluida en la solicitud respectiva y transmitir los datos al cliente solicitante (etapas **418-420).**

Cuando la comunicación comprende un informe de reputación, en una etapa **424,** el servidor **14** puede buscar datos de reputación asociados con la huella digital de la entidad incluida en el informe de reputación respectivo. Cuando el informe **73** indica un valor de reputación actual que indica menos confianza que la reputación histórica almacenada en la base de datos **16,** en una etapa **428** algunas realizaciones del servidor **14** de reputación pueden cambiar inmediatamente la entrada de la base de datos respectiva para incluir el valor del indicador de reputación recibido en el informe procedente del cliente **10.**

Cuando el informe **73** comprende un indicador de reputación indicativo de más confianza que el valor almacenado actualmente, en algunas realizaciones una etapa **430** puede agregar el informe **73** de reputación a una colección de informes recibidos de varios clientes. En una etapa **432,** el servidor **14** de reputación puede entonces determinar si se satisface una condición de actualización y actualizar la entrada de la base de datos sólo cuando se satisface la condición de actualización. La condición de actualización puede formularse según una limitación de tiempo y/o según un recuento de informes recibidos para cada huella digital de entidad individual. Por ejemplo, una actualización puede ocurrir solo después de que haya transcurrido un cierto intervalo de tiempo desde la última actualización del indicador de reputación correspondiente a la huella digital de la entidad respectiva. En otro ejemplo, la actualización puede ocurrir solo después de que haya transcurrido un cierto intervalo de tiempo desde la última notificación de seguridad con respecto a la entidad objetivo-respectiva. En una realización ejemplar en la que una alta reputación equivale a más confianza, cuando se satisface la condición de actualización, la reputación histórica de una entidad objetivo se actualiza a un valor igual al mínimo de todas las reputaciones informadas para la entidad objetivo-respectiva durante el último período de actualización.

Los sistemas y métodos ejemplares descritos anteriormente permiten proteger un sistema cliente, tal como un ordenador personal, tableta o teléfono inteligente, de software malicioso. En algunas realizaciones, un administrador de reputación se ejecuta al mismo tiempo que un motor anti-malware. El motor anti-malware realiza operaciones tales como detectar malware que se ejecuta en el sistema cliente respectivo y/o eliminar o inhabilitar dicho malware. Para cada entidad (por ejemplo, aplicación, proceso, script) que se ejecuta en el sistema cliente, el administrador de reputación puede transmitir un indicador de reputación al motor anti-malware, el indicador de reputación indica un nivel de confianza de que la entidad respectiva no es maliciosa.

En los sistemas de seguridad convencionales, las entidades de software se escanean y/o monitorean independientemente de su reputación. Por el contrario, en algunas realizaciones de la presente invención, el motor anti-malware puede dar un trato preferencial a las entidades de confianza. Por ejemplo, el motor anti-malware puede usar un protocolo computacionalmente menos costoso (por ejemplo, que requiere más ciclos de reloj del procesador y/o más memoria) para escanear/monitorear una entidad confiable, en comparación con una entidad no confiable o desconocida/no vista anteriormente. En uno de estos ejemplos, un subconjunto de reglas puede desactivarse al escanear/monitorear entidades confiables. Este enfoque puede mejorar sustancialmente el desempeño anti-malware, al reducir la carga computacional asociada con el escaneo/monitoreo de entidades confiables.

En algunas realizaciones de la presente invención, cada entidad ejecutable se ve como una combinación única de componentes/bloques de construcción. Ejemplos de tales bloques de construcción incluyen, entre otros, un ejecutable principal, una biblioteca compartida, un script y una sección de código inyectado. Cada combinación de componentes puede identificarse mediante una huella digital de entidad que comprende, por ejemplo, una combinación de valores hash de componentes individuales. A continuación, se puede asociar un indicador de reputación con cada huella digital de entidad. Cuando la composición de una entidad cambia (por ejemplo, cuando un proceso carga dinámicamente una biblioteca o recibe un fragmento de código inyectado), su huella digital cambia y también lo hace su reputación.

En algunas realizaciones, la reputación de una entidad cambia con el tiempo. Si bien una entidad no realiza ninguna acción sospechosa o indicativa de malware, su reputación puede cambiar hacia valores indicativos de mayor confianza. Por el contrario, cuando una entidad realiza una acción indicativa de malware o de algún otro modo relevante para la seguridad, su reputación puede verse degradada a valores que indiquen menos confianza. Dichos cambios en la reputación pueden guardarse en una memoria caché local y/o transmitirse a una base de datos de reputación central. Dichas configuraciones permiten que cualquier cambio en la reputación se propague rápidamente a otros procesos locales utilizando instancias de la biblioteca compartida respectiva y, además, a otros sistemas cliente conectados al servidor de reputación.

En algunas realizaciones, una caída en la reputación (que puede indicar una sospecha de malicia) se propaga relativamente rápido a las bases de datos de reputación y desde allí a otros sistemas de clientes, mientras que los aumentos en la reputación (que pueden indicar un aumento en la confianza) pueden tener efecto solo después de que haya transcurrido suficiente tiempo sin incidentes de seguridad, o después de que se haya informado que la entidad respectiva se comportó bien por un número suficiente de sistemas cliente.

Los sistemas y métodos descritos en la presente memoria pueden aplicarse fácilmente a una amplia variedad de software malicioso, incluidas las amenazas emergentes. Además, dado que el administrador de reputación opera

independientemente del motor anti-malware, el motor anti-malware puede actualizarse para incorporar nuevos métodos y procedimientos de escaneo/monitoreo, sin afectar el funcionamiento del administrador de reputación.

Será evidente para un experto en la técnica que las realizaciones anteriores pueden modificarse de muchas formas sin apartarse del alcance de la invención. Por consiguiente, el alcance de la invención debería estar determinado por las siguientes reivindicaciones y sus equivalentes legales.

REIVINDICACIONES

1. Un sistema cliente (10) que comprende al menos un procesador (32) de hardware configurado para ejecutar una entidad objetivo (80), un administrador (58) de reputación y un motor (56) anti-malware, en el que:

el administrador de reputación está configurado para:

en respuesta a la recepción de un primer indicador (60) de reputación de la entidad objetivo procedente de un servidor (14) de reputación, siendo el primer indicador de reputación indicativo de una probabilidad de que la entidad objetivo sea maliciosa, transmitir el indicador de reputación al motor anti-malware,

en respuesta a la recepción del primer indicador de reputación, actualizar el primer indicador de reputación determinando un segundo indicador de reputación de la entidad objetivo, difiriendo el segundo indicador de reputación del primer indicador de reputación por un cambio de reputación, y

en respuesta a la determinación del segundo indicador de reputación, transmitir el segundo indicador de reputación al motor anti-malware y al servidor de reputación,

en el que la determinación del segundo indicador de reputación comprende:

en respuesta a la recepción del primer indicador de reputación, determinar un primer intervalo de tiempo,

en respuesta a la determinación del primer intervalo de tiempo, determinar si la entidad objetivo ha realizado alguna de un conjunto de acciones predeterminadas durante el primer intervalo de tiempo,

en respuesta, si la entidad objetivo no ha realizado ninguna de las acciones predeterminadas durante el primer intervalo de tiempo, determinar el cambio de reputación para indicar una reducción en la probabilidad de que la entidad objetivo sea maliciosa, y

si la entidad objetivo ha realizado una primera acción del conjunto de acciones predeterminadas durante el primer intervalo de tiempo, determinar el cambio de reputación para indicar un aumento en la probabilidad de que la entidad objetivo sea maliciosa;

y en donde

el motor anti-malware está configurado para:

en respuesta a la recepción del primer indicador de reputación, emplear un primer protocolo para determinar si la entidad objetivo es maliciosa, y

en respuesta a la recepción del segundo indicador de reputación, emplear un segundo protocolo para determinar si la entidad objetivo es maliciosa, en donde el segundo protocolo es menos costoso computacionalmente que el primer protocolo cuando el segundo indicador de reputación indica una menor probabilidad de malicia en comparación con el primer indicador de reputación, y en el que el segundo protocolo es más costoso computacionalmente que el primer protocolo cuando el segundo indicador de reputación indica una mayor probabilidad de malicia en comparación con el primer indicador de reputación.

2. El sistema cliente de la reivindicación 1, en el que el administrador de reputación está configurado, además, en respuesta a la determinación del segundo indicador de reputación, para actualizar el segundo indicador de reputación determinando un tercer indicador de reputación de la entidad objetivo, difiriendo el tercer indicador de reputación del segundo indicador de reputación por otro cambio de reputación, en el que la determinación del tercer indicador de reputación comprende:

determinar un segundo intervalo de tiempo posterior al primer intervalo de tiempo;

en respuesta a la determinación del segundo intervalo de tiempo, determinar si la entidad objetivo ha realizado alguna de las acciones predeterminadas durante el segundo intervalo de tiempo;

en respuesta, si la entidad objetivo no ha realizado ninguna de las acciones predeterminadas durante el segundo intervalo de tiempo, determinar el otro cambio de reputación para indicar otra reducción en la probabilidad de que la entidad objetivo sea maliciosa; y

si la entidad objetivo ha realizado una segunda acción del conjunto de acciones predeterminadas, determinar el otro cambio de reputación para indicar otro aumento en la probabilidad de que la entidad objetivo sea maliciosa.

3. El sistema cliente de la reivindicación 2, en el que el tamaño del segundo intervalo de tiempo se determina de acuerdo con el tamaño del primer intervalo de tiempo.

4. El sistema cliente de la reivindicación 2, en el que el otro cambio de reputación se determina según un tamaño del primer intervalo de tiempo.

5. El sistema cliente de la reivindicación 1, en el que el administrador de reputación está configurado además para determinar el cambio de reputación de acuerdo con el tiempo transcurrido desde el lanzamiento de la entidad objetivo en el sistema de cliente.

6. El sistema cliente de la reivindicación 1, en el que el primer intervalo de tiempo se determina según un tiempo transcurrido desde el lanzamiento de la entidad objetivo en el sistema cliente.

7. El sistema de cliente de la reivindicación 1, en el que el primer intervalo de tiempo se determina según el primer indicador de reputación.

8. El sistema cliente de la reivindicación 1, en el que el primer intervalo de tiempo se determina según si la entidad objetivo ha realizado una segunda acción del conjunto de acciones predeterminadas antes del primer intervalo de tiempo.

9. El sistema cliente de la reivindicación 1, en el que el cambio de reputación se determina según un tipo de la primera acción.

10. El sistema cliente de la reivindicación 1, en el que el cambio de reputación se determina según si la entidad objetivo ha realizado una segunda acción antes de la primera acción.

11. El sistema cliente de la reivindicación 1, en el que el administrador de reputación está configurado, además, en respuesta a la determinación del segundo indicador de reputación, para actualizar otro indicador de reputación de otra entidad que se ejecuta en el sistema de cliente, comprendiendo la otra entidad un componente de la entidad objetivo, siendo el otro indicador de reputación indicativo de la probabilidad de que la otra entidad sea maliciosa.

12. El sistema cliente de la reivindicación 1, en el que la primera acción comprende que la entidad objetivo inyecte una sección de código en otra entidad que se ejecuta en el sistema cliente, y en el que el administrador de reputación se configura además, en respuesta a la determinación del tercer indicador de reputación, para determinar otro indicador de reputación de la otra entidad que se ejecuta en el sistema cliente, indicando el otro indicador de reputación que la otra entidad es tan probable que sea maliciosa como la entidad objetivo.

13. Un sistema (14) informático servidor que comprende al menos un procesador de hardware configurado para realizar transacciones de administración de la reputación con una pluralidad de sistemas cliente (10a, 10b, 10c), en el que una transacción de administración de la reputación comprende:

en respuesta a una solicitud recibida desde un sistema cliente de la pluralidad de sistemas cliente, el sistema cliente ejecuta una entidad objetivo, recuperando un primer indicador (60) de reputación de una entidad objetivo (80) desde una base de datos (16) de reputación de la entidad, siendo el primer indicador de reputación indicativo de una probabilidad de que la entidad objetivo sea maliciosa;

en respuesta a la recuperación del primer indicador de reputación, transmitir el primer indicador de reputación al sistema cliente;

en respuesta a la transmisión del primer indicador de reputación, recibir un segundo indicador de reputación de la entidad objetivo del sistema del cliente;

en respuesta a la recepción del segundo indicador de reputación, comparar el primer y segundo indicadores de reputación;

en respuesta, cuando el segundo indicador de reputación indica una probabilidad menor de que la entidad objetivo sea maliciosa que la indicada por el primer indicador de reputación, agregar el segundo indicador de reputación a una colección de indicadores de reputación recibidos desde la pluralidad de sistemas cliente, donde todos los miembros de la colección se determinan para instancias de la entidad objetivo;

en respuesta a la agregación del segundo indicador de reputación a la colección, determinar si se cumple una condición de actualización de reputación; y

en respuesta, cuando se cumple la condición de actualización, reemplazar el primer indicador de reputación en la base de datos de reputación por un indicador de reputación actualizado determinado según la colección;

en donde el segundo indicador de reputación difiere del primer indicador de reputación por un cambio de reputación, y donde la determinación del segundo indicador de reputación comprende emplear el sistema cliente para:

en respuesta a la recepción del primer indicador de reputación, determinar un primer intervalo de tiempo,

en respuesta a la determinación del primer intervalo de tiempo, determinar si la entidad objetivo ha realizado alguna de un conjunto de acciones predeterminadas durante el primer intervalo de tiempo,

en respuesta, si la entidad objetivo no ha realizado ninguna del conjunto de acciones predeterminadas durante el primer intervalo de tiempo, determinar el cambio de reputación para indicar una reducción en la probabilidad de que la entidad objetivo sea maliciosa, y

si la entidad objetivo ha realizado una primera acción del conjunto de acciones predeterminadas, determinar el cambio de reputación para indicar un aumento en la probabilidad de que la entidad objetivo sea maliciosa.

14. El sistema informático servidor de la reivindicación 13, en el que determinar si se satisface la condición de actualización comprende determinar el tiempo transcurrido desde que se agregó el primer miembro a la colección.

15. El sistema informático servidor de la reivindicación 13, en el que determinar si se satisface la condición de actualización comprende determinar un recuento de los miembros de la colección.

16. El sistema informático servidor de la reivindicación 13, en el que la determinación del indicador de reputación actualizado comprende formular el indicador de reputación actualizado para indicar una probabilidad más alta de que la entidad objetivo sea malintencionada de todos los miembros de la colección.

17. El sistema informático servidor de la reivindicación 13, configurado, además, en respuesta a la recepción del segundo indicador de reputación, para recibir del sistema cliente un tercer indicador de reputación determinado para la entidad objetivo, difiriendo el tercer indicador de reputación del segundo indicador de reputación por otro cambio de reputación, y en el que la determinación del tercer indicador de reputación por parte del sistema cliente comprende:

determinar un segundo intervalo de tiempo posterior al primer intervalo de tiempo;

en respuesta a la determinación del segundo intervalo de tiempo, determinar si la entidad objetivo ha realizado alguna de las acciones predeterminadas durante el segundo intervalo de tiempo;

en respuesta, si la entidad objetivo no ha realizado ninguna del conjunto de acciones predeterminadas durante el segundo intervalo de tiempo, determinar el otro cambio de reputación para indicar otra reducción en la probabilidad de que la entidad objetivo sea maliciosa; y

si la entidad objetivo ha realizado una segunda acción del conjunto de acciones predeterminadas, determinar el otro cambio de reputación para indicar otro aumento en la probabilidad de que la entidad objetivo sea maliciosa.

18. El sistema informático servidor de la reivindicación 13, en el que el cambio de reputación se determina según el tiempo transcurrido desde el lanzamiento de la entidad objetivo en el sistema cliente.

19. El sistema informático servidor de la reivindicación 13, en el que el primer intervalo de tiempo se determina según un tiempo transcurrido desde el lanzamiento de la entidad objetivo en el sistema cliente.

20. El sistema informático servidor de la reivindicación 13, en el que el primer intervalo de tiempo se determina según el primer indicador de reputación.

21. El sistema informático servidor de la reivindicación 13, en el que el primer intervalo de tiempo se determina según si la entidad objetivo ha realizado una segunda acción del conjunto de acciones predeterminadas antes del primer intervalo de tiempo.

22. Un medio legible por ordenador no transitorio que almacena un conjunto de instrucciones que, cuando son ejecutadas por un procesador (32) de hardware de un sistema cliente, hacen que el sistema cliente (10) forme un administrador (58) de reputación y un motor (56) anti-malware, en el que:

el sistema cliente está configurado para ejecutar una entidad objetivo;

el administrador (58) de reputación está configurado para:

en respuesta a la recepción de un primer indicador de reputación de la entidad objetivo de un servidor de reputación, siendo el primer indicador de reputación indicativo de una probabilidad de que la entidad objetivo sea maliciosa, transmitir el indicador de reputación al motor anti-malware,

en respuesta a la recepción del primer indicador de reputación, actualizar el primer indicador de reputación determinando un segundo indicador de reputación de la entidad objetivo, difiriendo el segundo indicador de reputación del primer indicador de reputación por un cambio de reputación, y

en respuesta a la determinación del segundo indicador de reputación, transmitir el segundo indicador de reputación al motor anti-malware y al servidor de reputación,

en el que la determinación del segundo indicador de reputación comprende:

en respuesta a la recepción del primer indicador de reputación, determinar un primer intervalo de tiempo,

en respuesta a la determinación del primer intervalo de tiempo, determinar si la entidad objetivo ha realizado alguna de un conjunto de acciones predeterminadas durante el primer intervalo de tiempo,

en respuesta, si la entidad objetivo no ha realizado ninguna de las acciones predeterminadas durante el primer intervalo de tiempo, determinar el cambio de reputación para indicar una reducción en la probabilidad de que la entidad objetivo sea maliciosa, y

si la entidad objetivo ha realizado una primera acción del conjunto de acciones predeterminadas durante el primer intervalo de tiempo, determinar el cambio de reputación para indicar un aumento en la probabilidad de que la entidad objetivo sea maliciosa;

y en donde

el motor (56) anti-malware está configurado para:

en respuesta a la recepción del primer indicador de reputación, emplear un primer protocolo para determinar si la entidad objetivo es maliciosa, y

en respuesta a la recepción del segundo indicador de reputación, emplear un segundo protocolo para determinar si la entidad objetivo es maliciosa, en donde el segundo protocolo es menos costoso computacionalmente que el primer protocolo cuando el segundo indicador de reputación indica una menor probabilidad de malicia en comparación con el primer indicador de reputación, y en el que el segundo protocolo es más costoso computacionalmente que el primer protocolo cuando el segundo indicador de reputación indica una mayor probabilidad de malicia en comparación con el primer indicador de reputación.

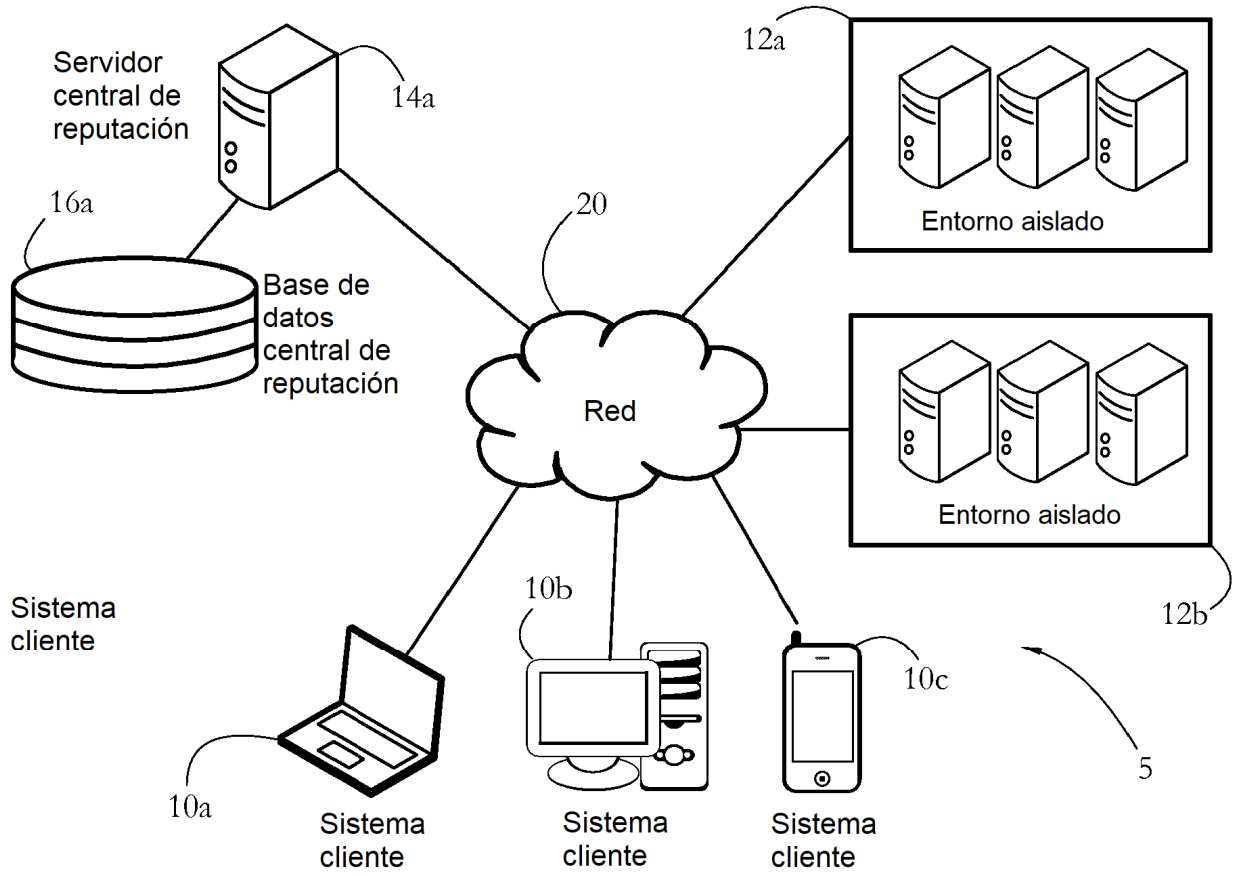
Servidor central de reputación
14a
16a
Base de datos central de reputación
20
Red
12a
Entorno aislado
Entorno aislado
12b
Sistema cliente
10a
Sistema cliente
10b
Sistema cliente
10c
Sistema cliente
5

FIG. 1

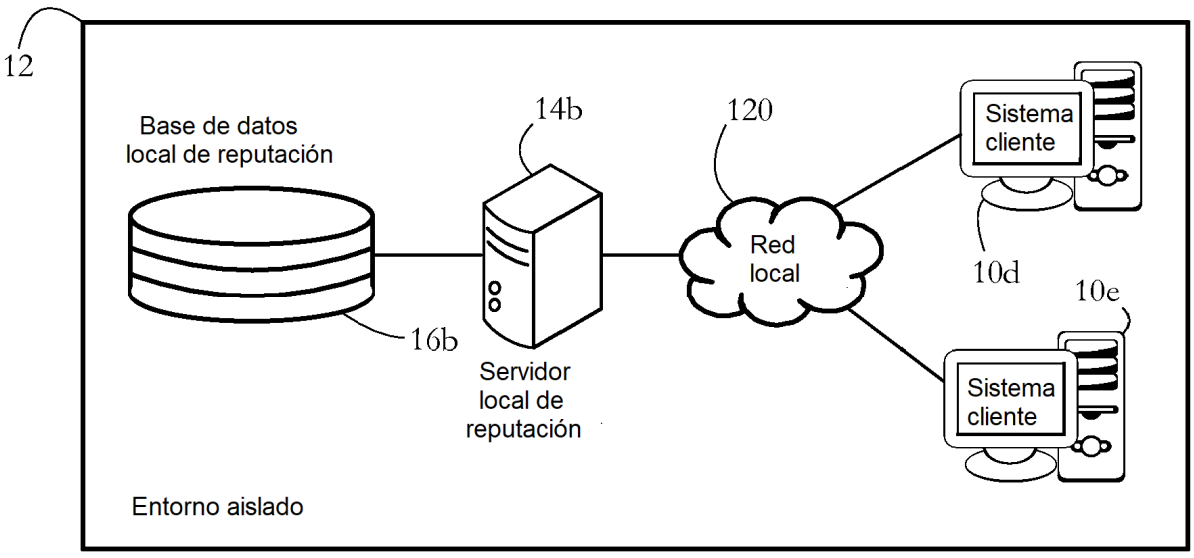
12
Base de datos local de reputación
14b
16b
Servidor local de reputación
120
Red local
Sistema cliente
10d
Sistema cliente
10e
Entorno aislado

FIG. 2

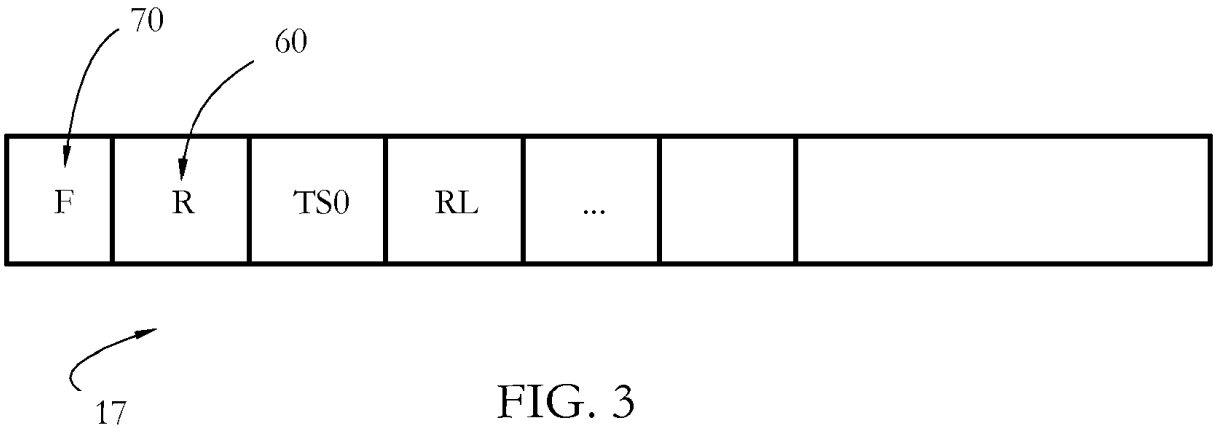
70
60
F
R
TS0
RL
...
17

FIG. 3

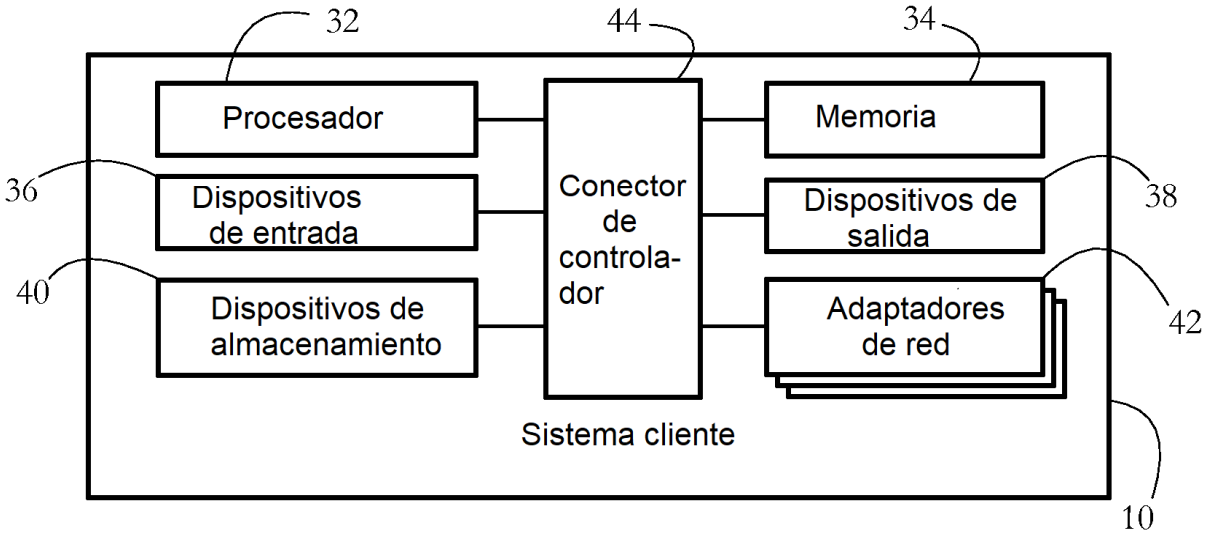
32
44
34
Procesador
Memoria
36
Dispositivos de entrada
Conector de controla-dor
Dispositivos de salida
38
40
Dispositivos de almacenamiento
Adaptadores de red
42
Sistema cliente
10

FIG. 4-A

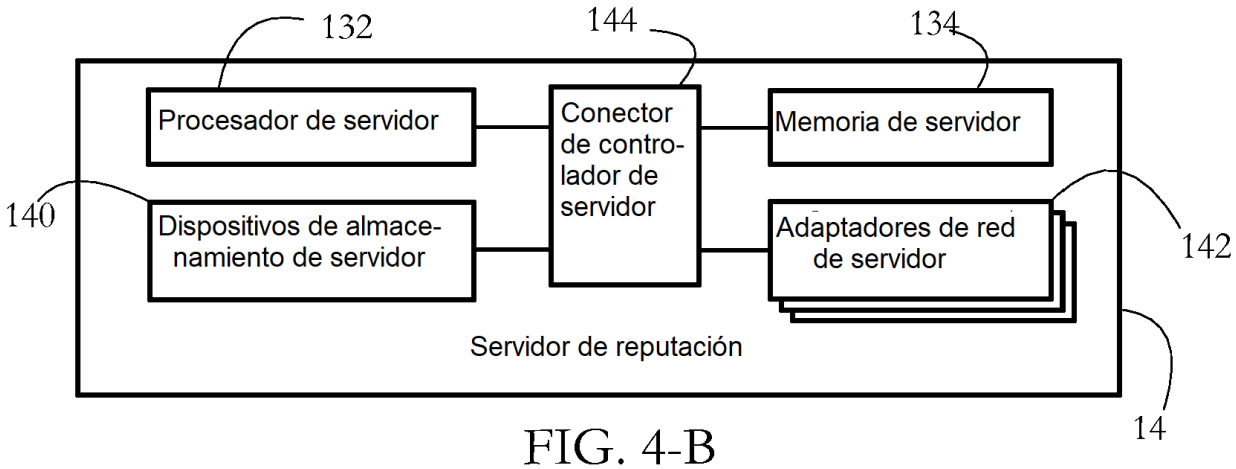
132
144
134
Procesador de servidor
Conector de contro-lador de servidor
Memoria de servidor
140
Dispositivos de almace-namiento de servidor
Adaptadores de red de servidor
142
Servidor de reputación
14

FIG. 4-B

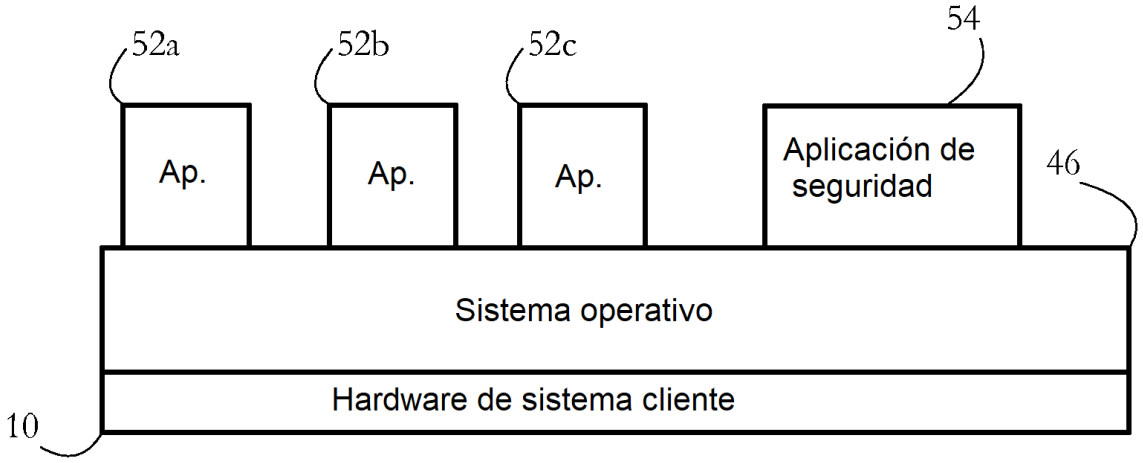
52a
52b
52c
54
Ap.
Ap.
Ap.
Aplicación de seguridad
46
Sistema operativo
Hardware de sistema cliente
10

FIG. 5

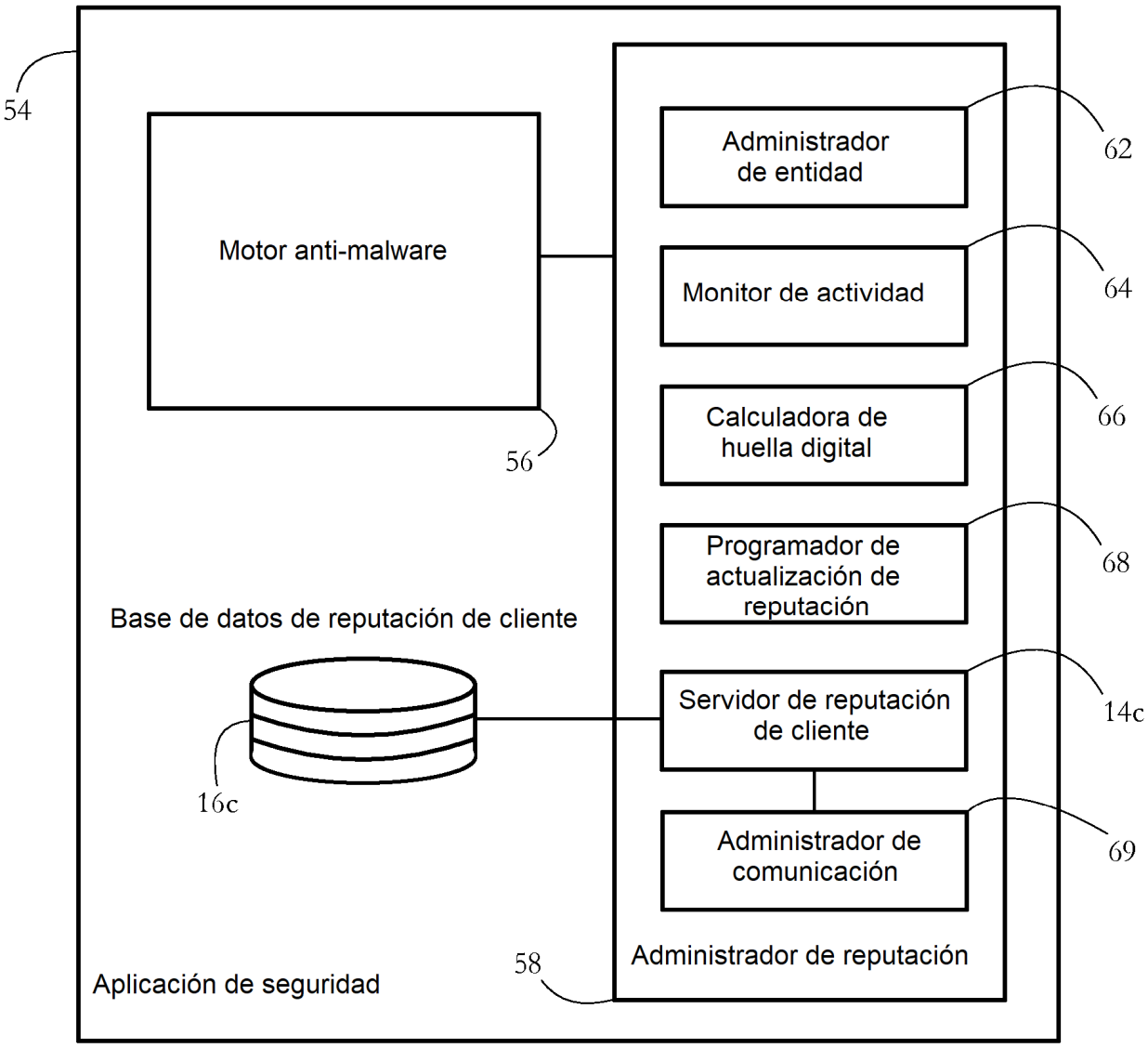
54
Motor anti-malware
56
Administrador de entidad
62
Monitor de actividad
64
Calculadora de huella digital
66
Programador de actualización de reputación
68
Base de datos de reputación de cliente
16c
Servidor de reputación de cliente
14c
Administrador de comunicación
69
Administrador de reputación
58
Aplicación de seguridad

FIG. 6

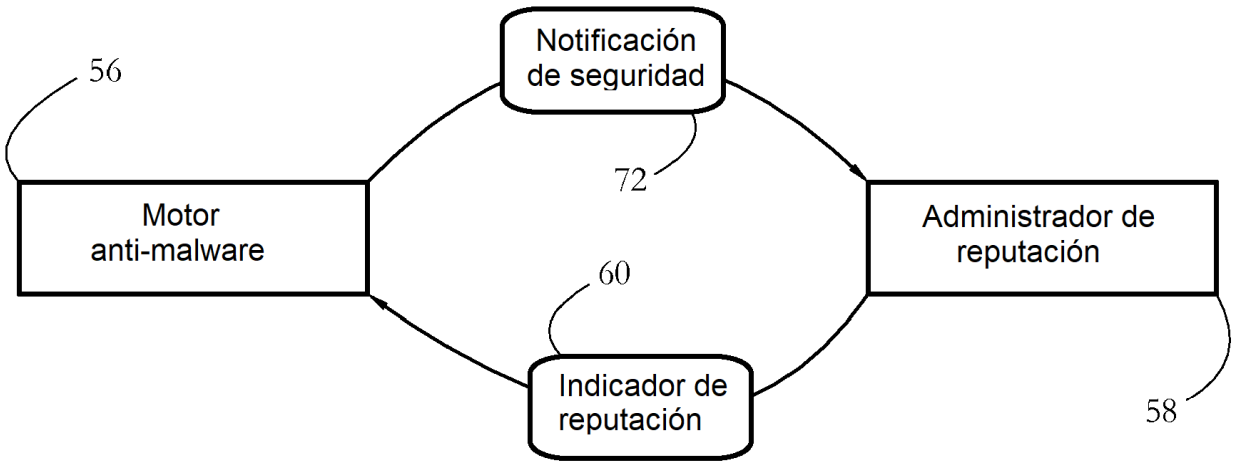
Notificación de seguridad
56
72
Motor anti-malware
Administrador de reputación
60
Indicador de reputación
58

FIG. 7

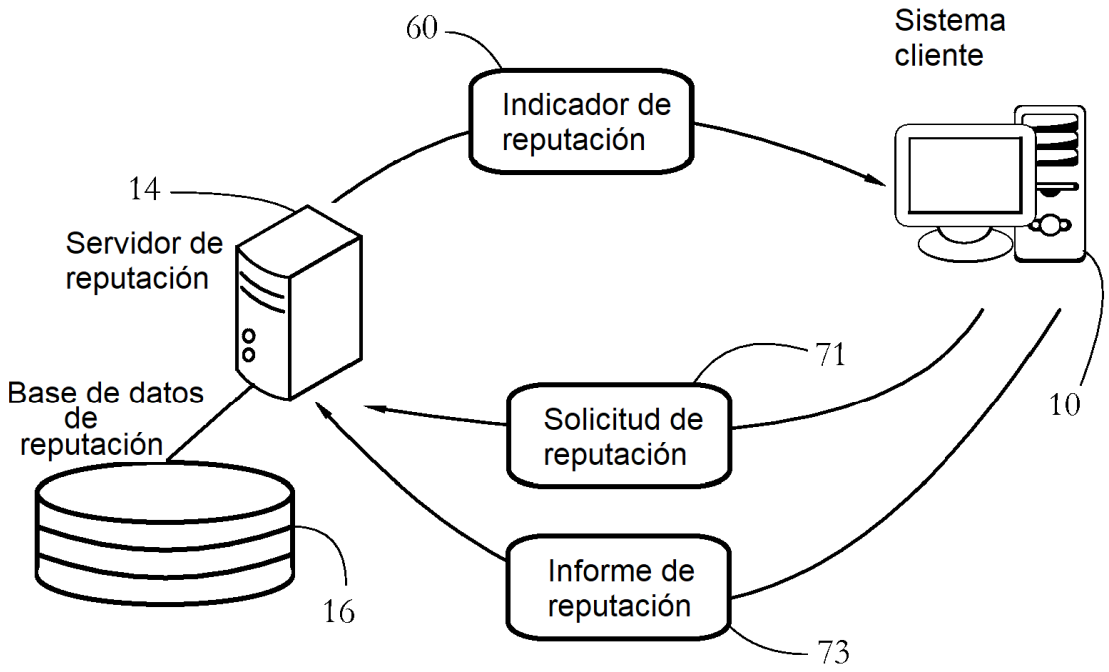
60
Indicador de reputación
Sistema cliente
14
Servidor de reputación
71
Base de datos de reputación
Solicitud de reputación
10
Informe de reputación
16
73

FIG. 8

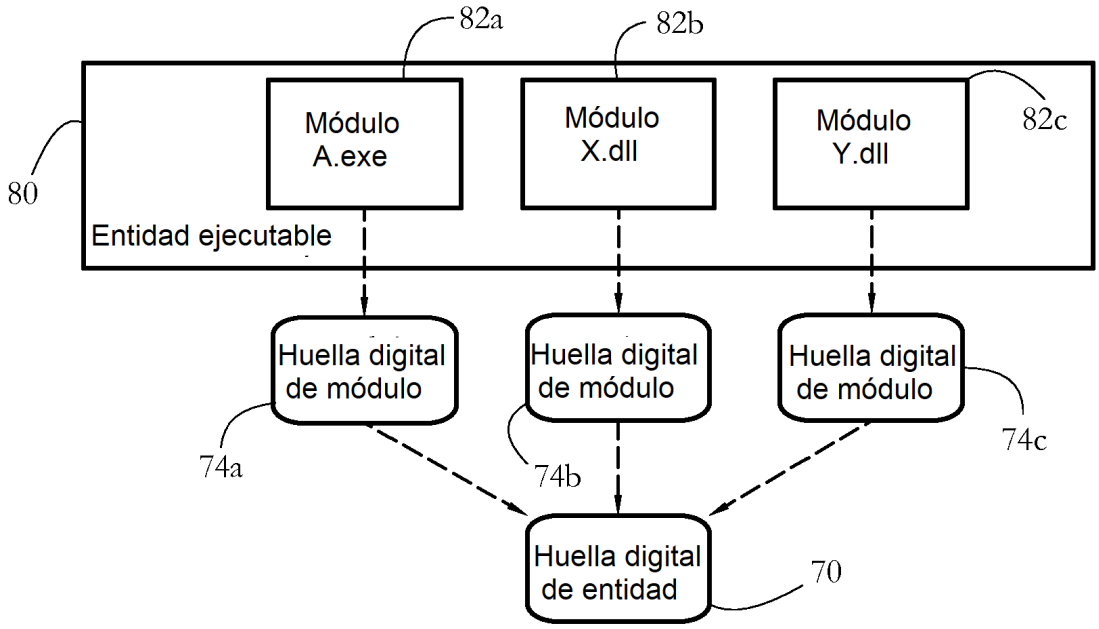
82a
82b
82c
Módulo A.exe
Módulo X.dll
Módulo Y.dll
80
Entidad ejecutable
Huella digital de módulo
Huella digital de módulo
Huella digital de módulo
74a
74b
74c
Huella digital de entidad
70

FIG. 9

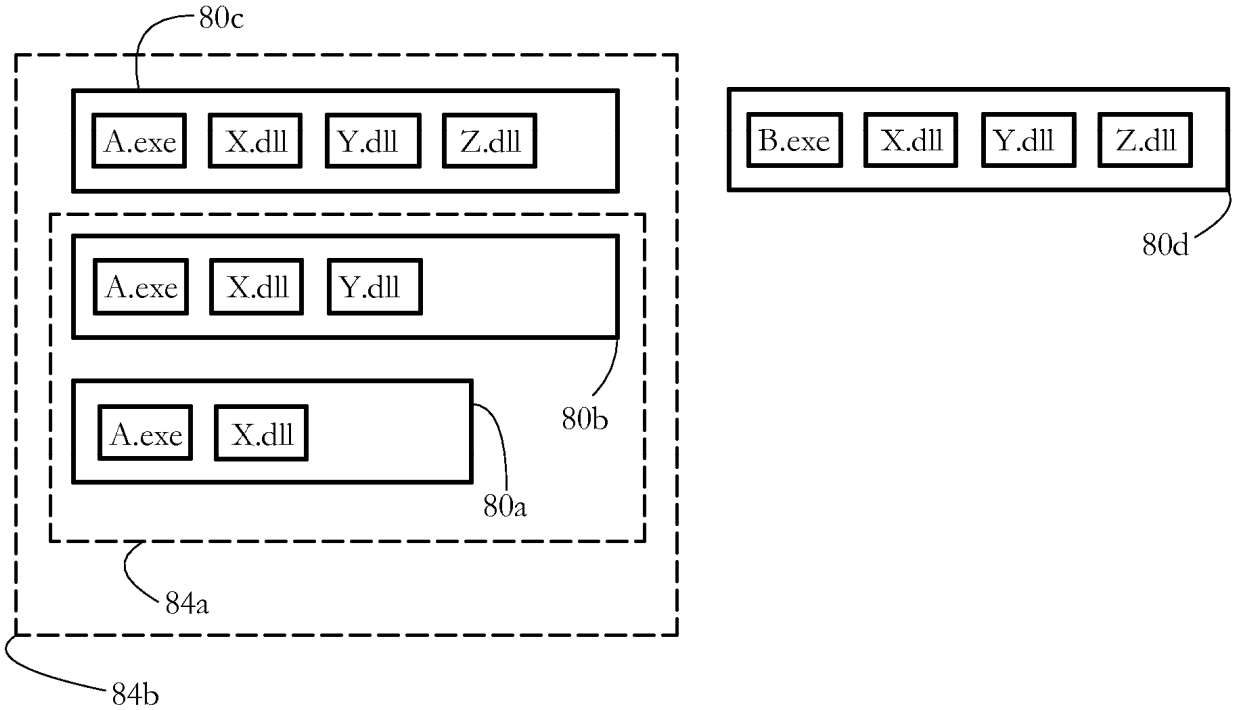
80c
A.exe
X.dll
Y.dll
Z.dll
A.exe
X.dll
Y.dll
80b
A.exe
X.dll
80a
84a
84b
B.exe
X.dll
Y.dll
Z.dll
80d

FIG. 10

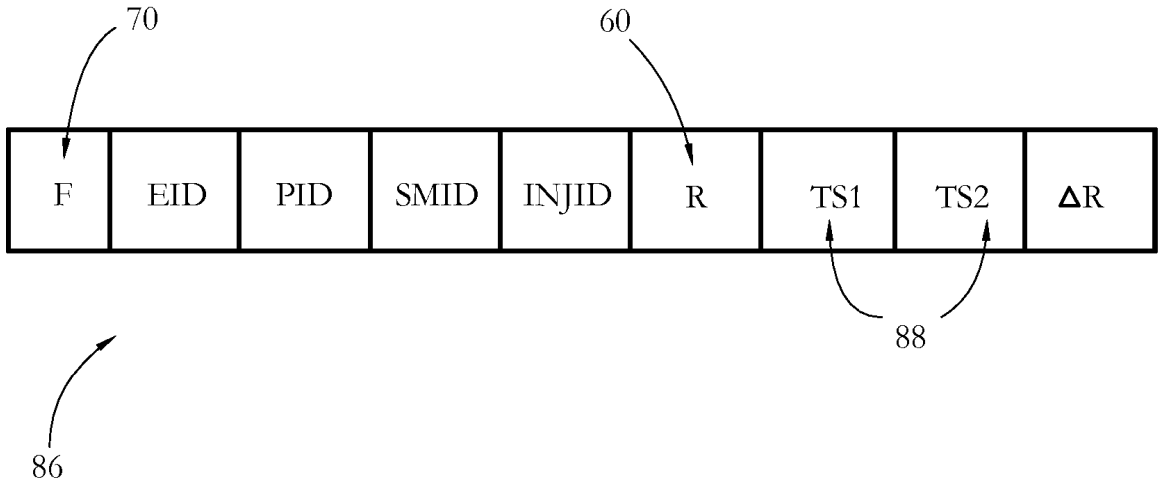

FIG. 11

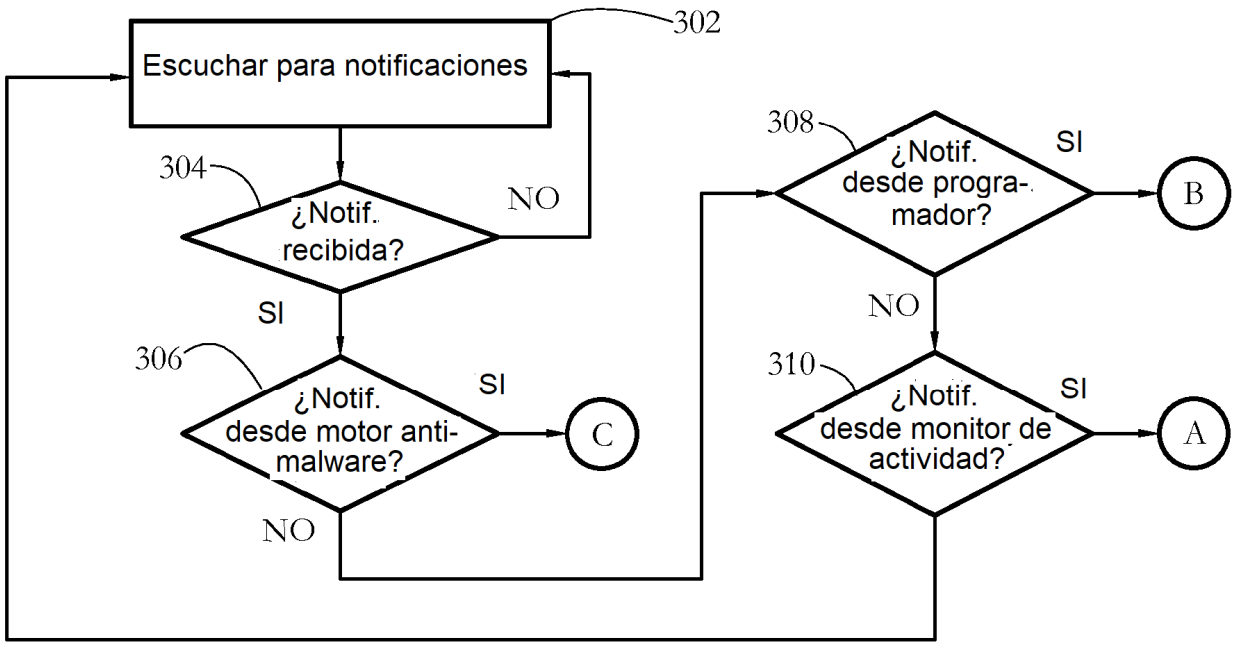

FIG. 12-A

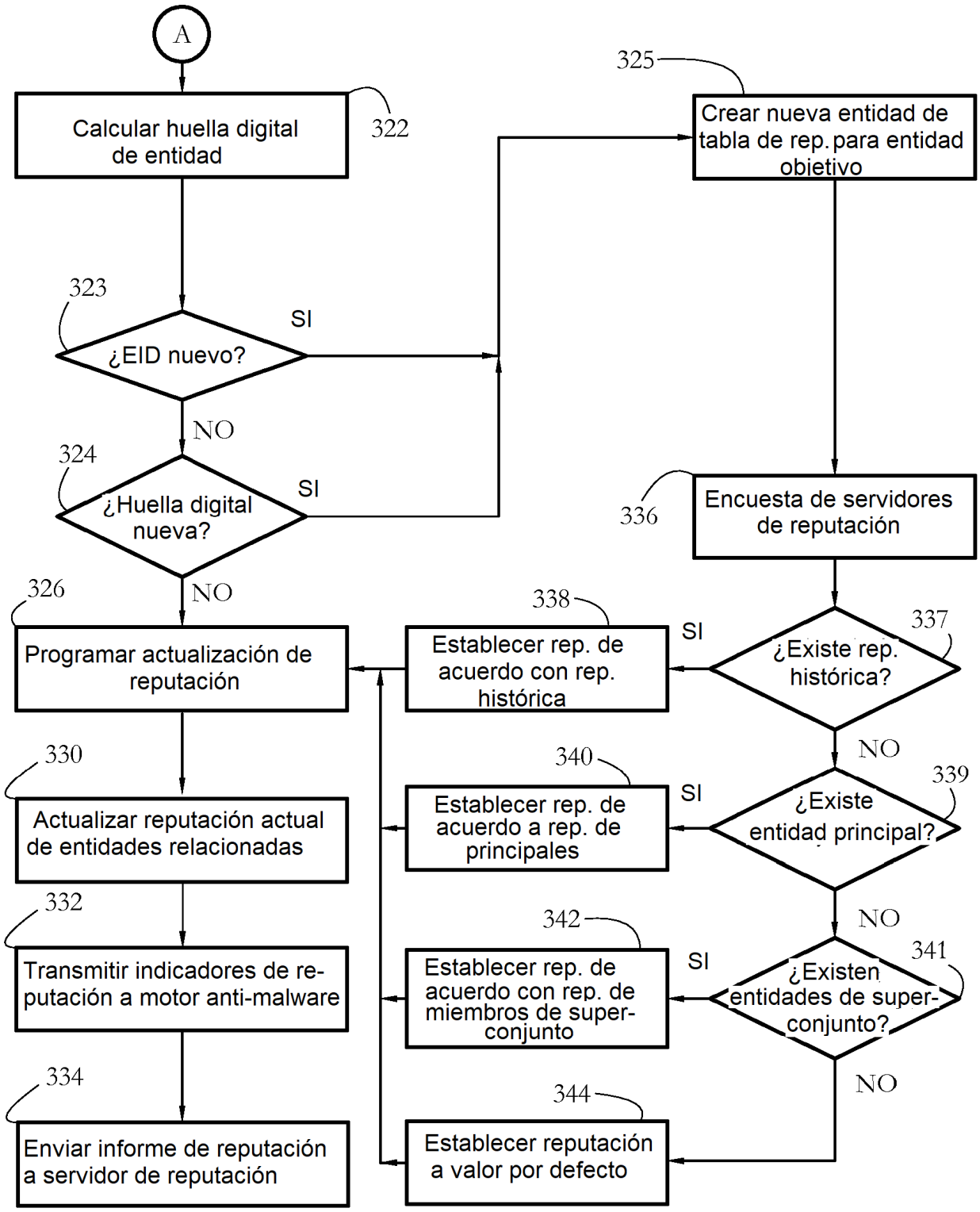
A
Calcular huella digital de entidad
322
323
¿EID nuevo?
SI
NO
324
¿Huella digital nueva?
SI
NO
325
Crear nueva entidad de tabla de rep. para entidad objetivo
336
Encuesta de servidores de reputación
337
¿Existe rep. histórica?
SI
338
Establecer rep. de acuerdo con rep. histórica
NO
339
¿Existe entidad principal?
SI
340
Establecer rep. de acuerdo a rep. de principales
NO
341
¿Existen entidades de super-conjunto?
SI
342
Establecer rep. de acuerdo con rep. de miembros de super-conjunto
NO
344
Establecer reputación a valor por defecto
326
Programar actualización de reputación
330
Actualizar reputación actual de entidades relacionadas
332
Transmitir indicadores de reputación a motor anti-malware
334
Enviar informe de reputación a servidor de reputación

FIG. 12-B

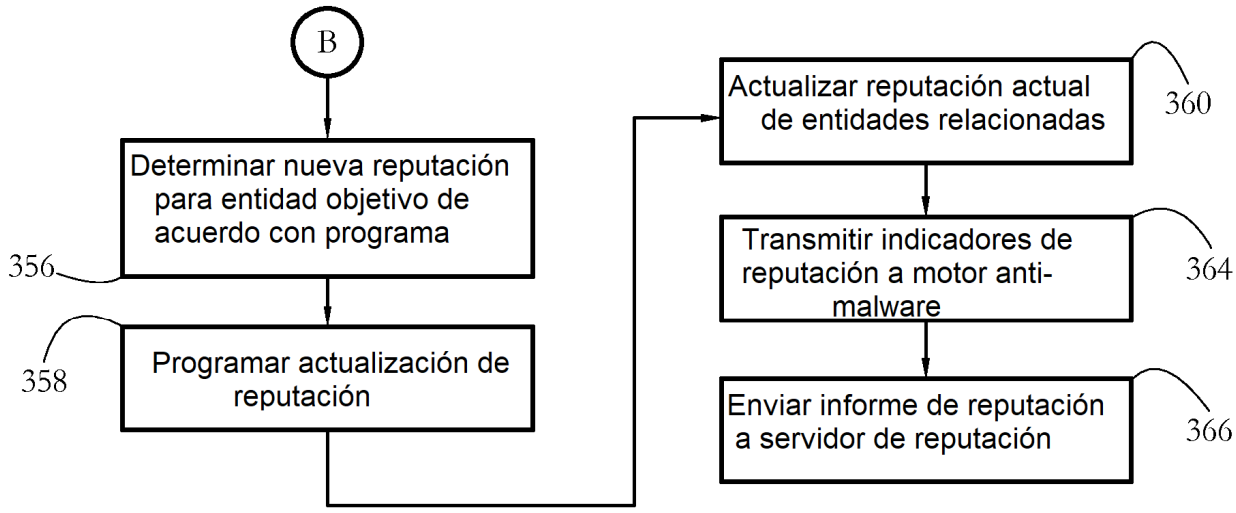

FIG. 12-C

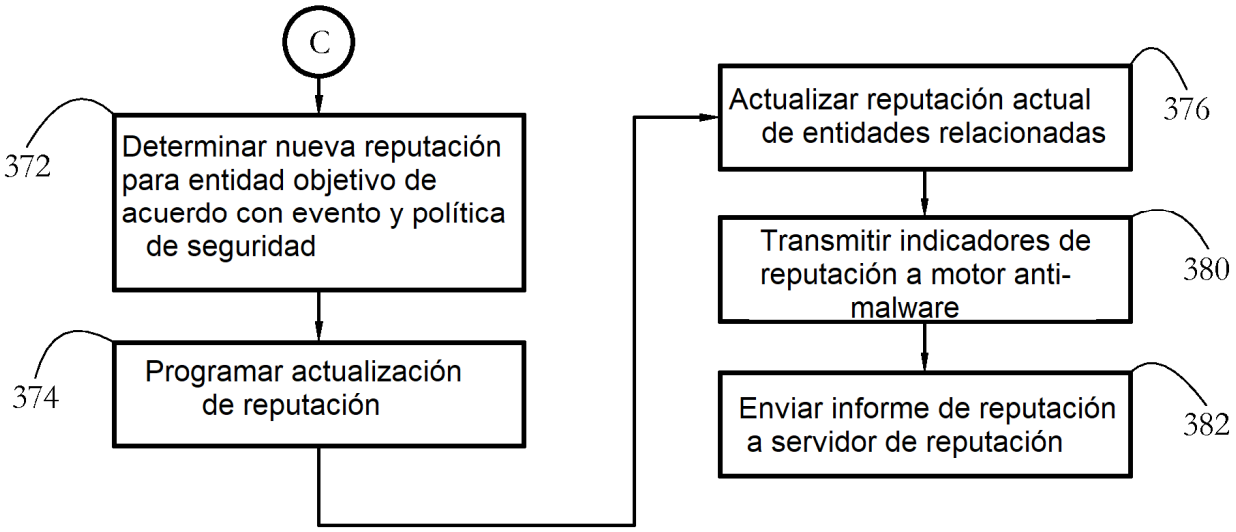

FIG. 12-D

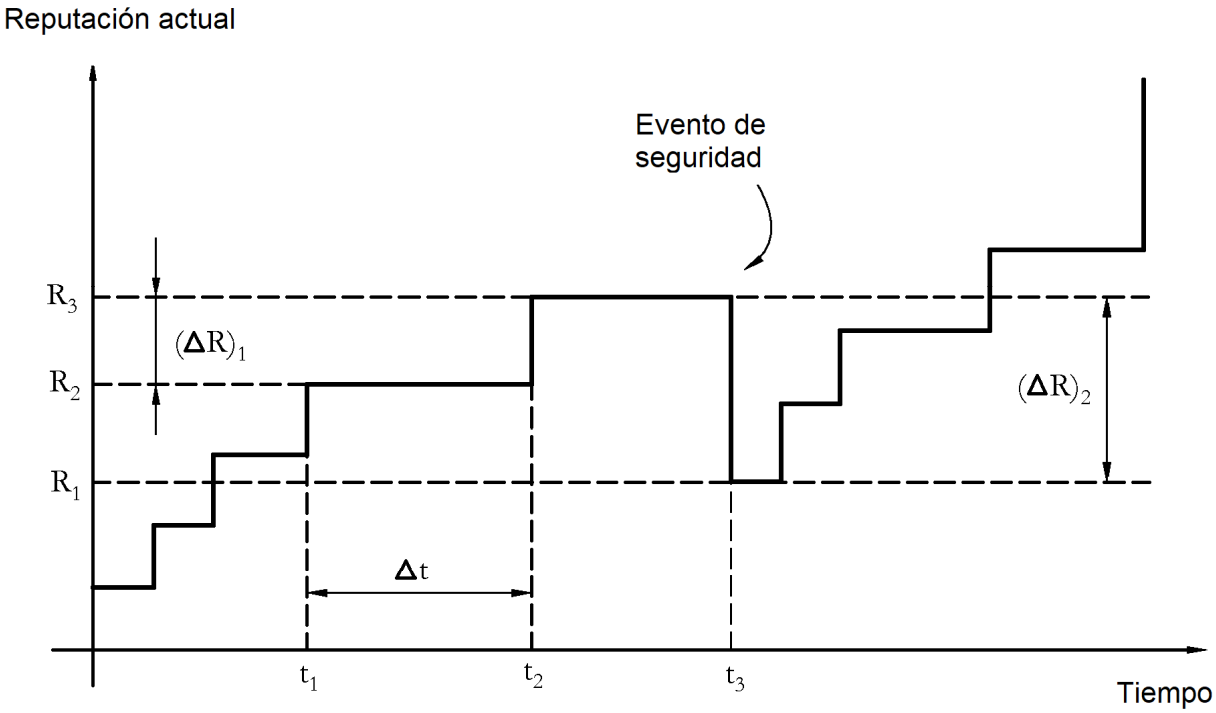
Reputación actual
Evento de seguridad
R3
R2
R1
(ΔR)1
(ΔR)2
Δt
t1
t2
t3
Tiempo

FIG. 13

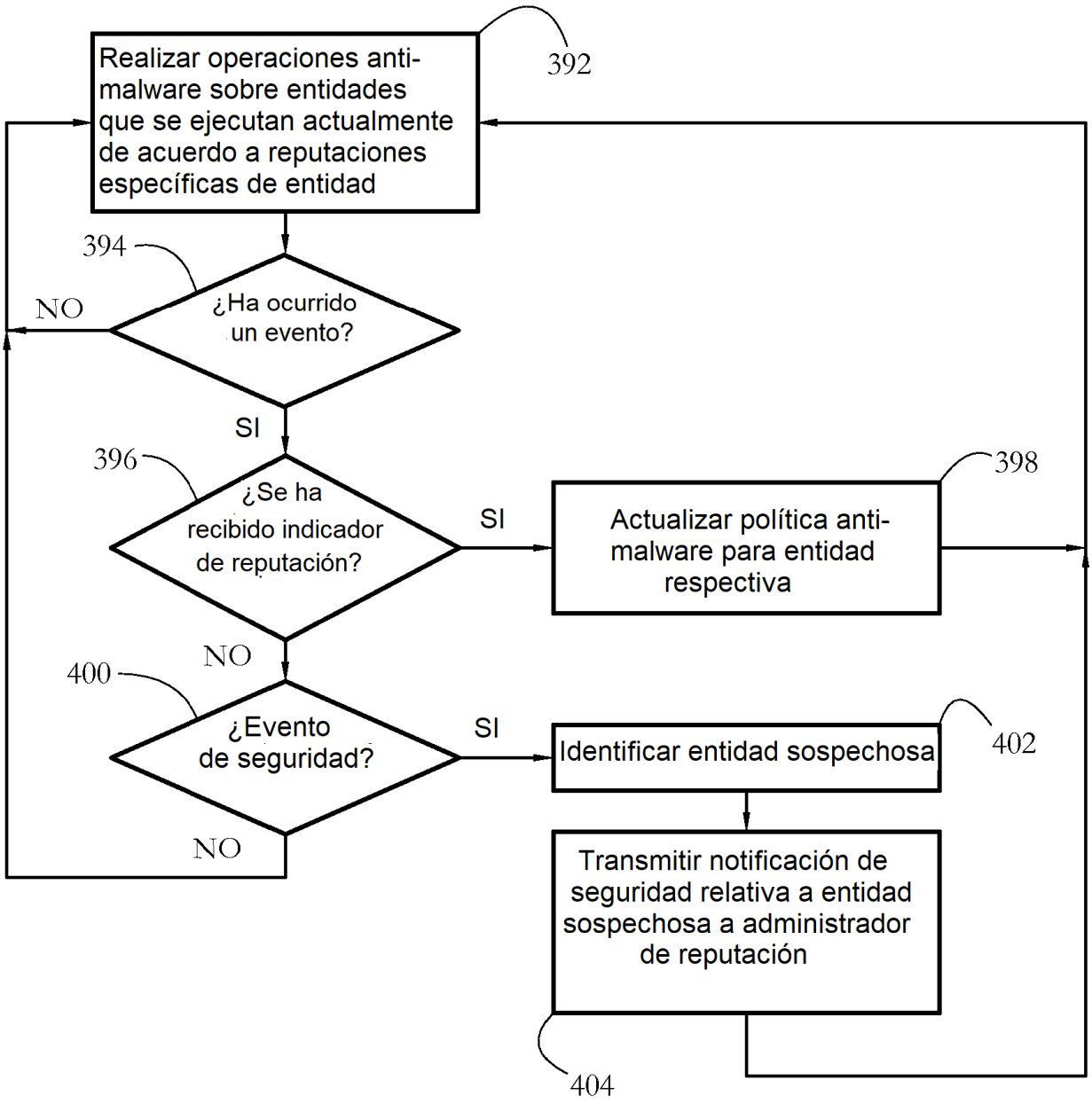
Realizar operaciones anti-malware sobre entidades que se ejecutan actualmente de acuerdo a reputaciones específicas de entidad
392
394
¿Ha ocurrido un evento?
NO
SI
396
¿Se ha recibido indicador de reputación?
SI
398
Actualizar política anti-malware para entidad respectiva
NO
400
¿Evento de seguridad?
SI
Identificar entidad sospechosa
402
NO
Transmitir notificación de seguridad relativa a entidad sospechosa a administrador de reputación
404

FIG. 14

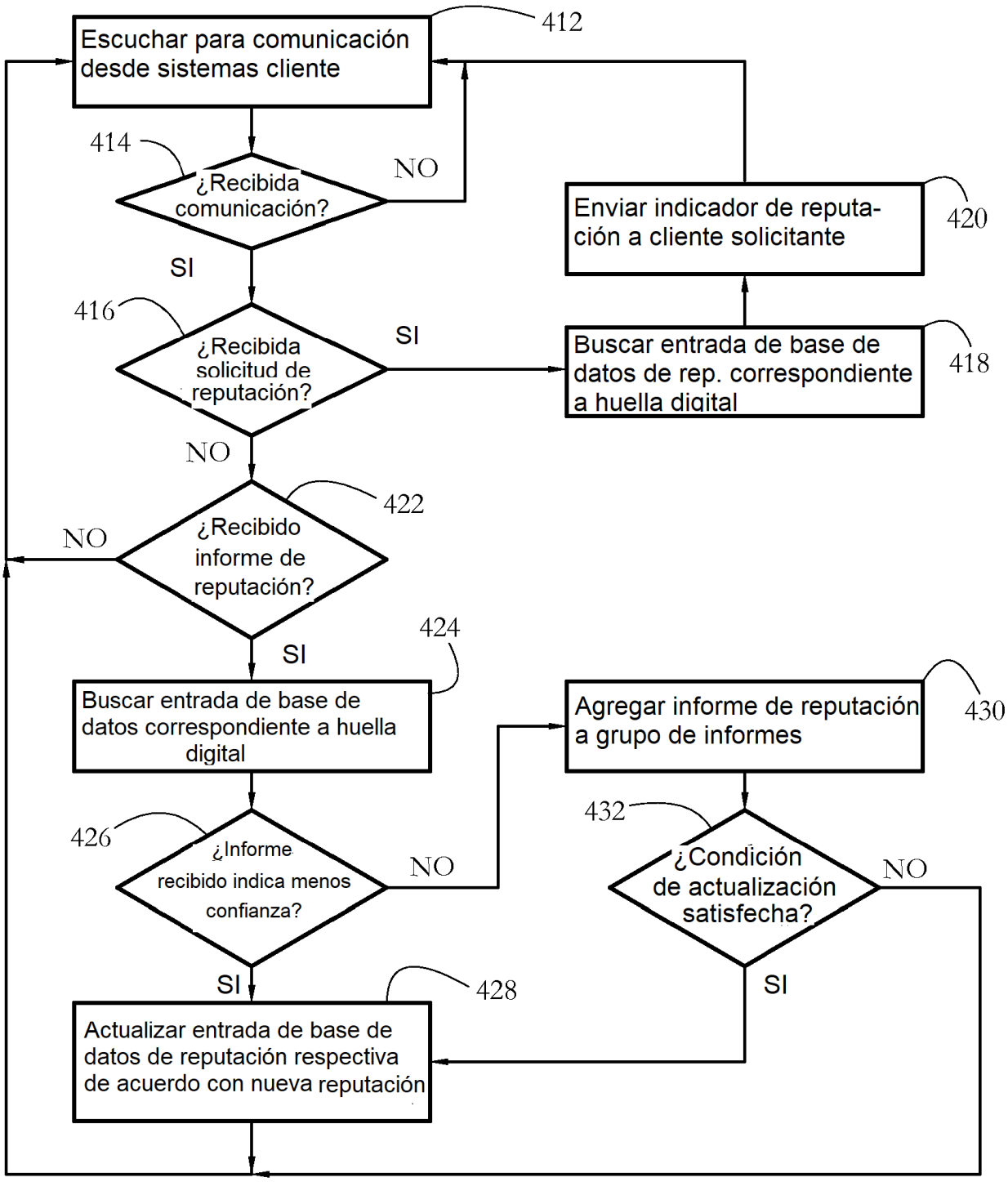
Escuchar para comunicación desde sistemas cliente
412
414
¿Recibida comunicación?
NO
SI
416
¿Recibida solicitud de reputación?
SI
Buscar entrada de base de datos de rep. correspondiente a huella digital
418
Enviar indicador de reputación a cliente solicitante
420
NO
422
¿Recibido informe de reputación?
NO
SI
424
Buscar entrada de base de datos correspondiente a huella digital
426
¿Informe recibido indica menos confianza?
NO
SI
428
Actualizar entrada de base de datos de reputación respectiva de acuerdo con nueva reputación
Agregar informe de reputación a grupo de informes
430
432
¿Condición de actualización satisfecha?
NO
SI

FIG. 15