(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 997 633**

(51) Int. Cl.:

H04L 9/28 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **12.06.2009 PCT/US2009/047161**

(87) Fecha y número de publicación internacional: **07.01.2010 WO10002568**

(96) Fecha de presentación y número de la solicitud europea: **12.06.2009 E 09774020 (3)**

(97) Fecha y número de publicación de la concesión europea: **02.10.2024 EP 2297898**

(54) Título: **Sistema y método de cognición de datos que incorpora protección de seguridad autónoma**

(30) Prioridad:

30.06.2008 US 164844

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
17.02.2025

(73) Titular/es:

SIEBEN SEVEN, LLC (100.00%)
9020 Alton Parkway
Silver Spring, Maryland, US

(72) Inventor/es:

BURGESS, SHELIA, JEAN y
BURGESS, GEORGE, G.

(74) Agente/Representante:

RUO, Alessandro

Aviso: En el plazo de nueve meses a contar desde la fecha de publicación en el Boletín Europeo de Patentes, de la mención de concesión de la patente europea, cualquier persona podrá oponerse ante la Oficina Europea de Patentes a la patente concedida. La oposición deberá formularse por escrito y estar motivada; sólo se considerará como formulada una vez que se haya realizado el pago de la tasa de oposición (art. 99.1 del Convenio sobre Concesión de Patentes Europeas).

DESCRIPCIÓN

Sistema y método de cognición de datos que incorpora protección de seguridad autónoma

Referencia cruzada a solicitudes relacionadas

[0001] Esta solicitud es una solicitud de continuación parcial de la solicitud de patente de EE. UU. en trámite junto con la presente con número de serie 11/968.509 presentada el 2 de enero de 2008, que es una solicitud de continuación parcial de la solicitud de patente de EE. UU. con número de serie 11/281.198 presentada el 16 de noviembre de 2005, que está abandonada en la actualidad, que era una solicitud de continuación de la solicitud de patente de EE. UU. con número de serie 10/056.246 presentada el 24 de enero de 2002, que está abandonada en la actualidad, que era una solicitud de continuación parcial de la solicitud de patente de EE. UU. con número de serie 09/293.041 presentada el 16 de abril de 1999, que es en la actualidad la patente de EE. UU. con número 6.359.970, que reivindica el beneficio de la prioridad de la solicitud provisional de EE. UU. con número de serie 60.103.653, presentada el 9 de octubre de 1998 y la solicitud provisional de EE. UU. con número de serie 60/096.594 presentada el 14 de agosto de 1998, y se hace referencia por la presente a las divulgaciones de todas ellas.

Aviso de derechos de autor

[0002] Este documento de patente contiene información y material sujetos a protección de derechos de autor.

Campo de la invención

[0003] Los aspectos de la presente invención se refieren en general a un sistema y a una metodología para la cognición de datos que incorpora protección de seguridad autónoma. Más particularmente, la invención se refiere a datos cognitivos de sistema y metodología que realizan análisis, se autogestionan, aseguran su entorno, evalúan comportamiento, detectan problemas de seguridad, se adaptan, alertan al creador de una situación urgente y proporcionan trazabilidad.

Antecedentes de la invención

[0004] La sociedad se ve bombardeada por ciberdelincuencia maliciosa. El robo de datos personales y corporativos, así como la alteración de datos, plagan nuestra dependencia de la tecnología informática. La Unidad de Negocio de Seguridad y Documentos Inteligentes de EE. UU. informó que se calcula que 13,3 personas son víctimas de fraude documental y de identidad cada 60 segundos, con casi siete millones de víctimas al año. Las redes robot y los piratas informáticos comprometen las redes para robar datos. La ciberdelincuencia es difícil de rastrear. Un delincuente informático puede usar ordenadores de cibercafés abiertos, moviéndose de un servidor a otro, cambiando de proveedor de Internet, usando información falsa para inscribirse, y puede robar el servicio de puntos de acceso inalámbrico no seguros.

[0005] Una vez se ha penetrado en las redes, los medios de seguridad para proteger datos tales como cifrado, protocolos de seguridad, acceso a datos y esquemas de autenticación no son suficientes. Está ampliamente aceptado que el cifrado de discos protege datos sensibles cuando se produce una apropiación indebida. Sin embargo, investigadores de la Universidad de Princeton mostraron que, incluso cuando se cifran, los datos pueden leerse fácilmente sin necesidad de acceso físico al ordenador. La lucha contra la ciberdelincuencia y el ciberterrorismo supone una honda preocupación entre los funcionarios federales, que se preguntan "cuando nuestras redes son atacadas y quedan inutilizadas, ¿cómo recuperamos el acceso a nuestros datos?". Solo el Pentágono registró 1.300 intrusiones con éxito en 2005. Piratas informáticos chinos penetraron en ordenadores del Departamento de Estado de EE. UU., cientos de los cuales tuvieron que sustituirse o ponerse sin conexión durante meses.

[0006] Los sistemas informáticos de empresa son protegidos por múltiples capas de seguridad que incluyen el cifrado de datos, la gestión de derechos digitales (DRM) y la gestión de derechos empresariales (ERM). Estas soluciones centradas en el servidor requieren una infraestructura de gestión de acceso tal como una comunicación de servidor empresarial o de licencias para autorizar el acceso a datos. Sin embargo, una conducta inapropiada de los empleados y acciones no deliberadas, como errores y omisiones, son la mayor causa de vulneraciones de seguridad de datos. La actividad delictiva puede tener lugar, y tiene lugar de hecho, dentro de empresas y organismos. Un delincuente tiene un acceso fácil más allá de las medidas de seguridad en vigor. Los robos de portátiles recientes y de alta repercusión mediática por integrantes de la propia organización incluyen un ordenador de la Administración de Veteranos que contenía información acerca de 26 millones de veteranos y un portátil de la Universidad de California-Berkeley con datos de más de 98.000 alumnos de posgrado, así como otros.

[0007] Además, las incidencias de emergencia que requieran que personal de primera intervención y otras agencias gubernamentales resuelvan un incidente a nivel nacional como se define en el Sistema de Gestión de Incidentes Nacionales (NIMS) del Departamento de Seguridad Nacional de EE. UU., pueden requerir el uso de datos clasificados. Las preocupaciones en el apoyo al NIMS son la pérdida de control de instanciaciones de datos clasificados que se compartieron durante el incidente.

[0008] Los documentos inteligentes son documentos electrónicos interactivos que suelen requerir acceso a un servidor web o de red. La dependencia de la red hace que estas soluciones sean vulnerables a vulneraciones de seguridad. Dado que, incluso si el usuario está autorizado a acceder a los datos, puede que los datos no estén aún protegidos. Tras abrir los datos o el documento, el entorno informático en el que se abrirán estos puede no ser seguro. Este sistema sigue dependiendo de la seguridad de red y de software de terceros, tal como protectores antivirus, protección antispyware y de cortafuegos. Los piratas informáticos podrían vulnerar la red, las soluciones de terceros podrían no detectar la última ciberamenaza o el usuario podría no tener la última actualización de seguridad.

[0009] Es muy deseable proporcionar a los usuarios la capacidad de limitar su exposición a la ciberdelincuencia y a las vulneraciones de datos, y proteger los datos en donde, incluso si un delincuente tiene éxito en superar las barreras de seguridad de red y obtiene una instanciación de los datos, será en vano. En lugar de depender de recursos externos en arquitecturas centradas en servidores de aplicaciones, existe la necesidad de que los propios datos sean inteligentes y autónomos. Los propios datos necesitan evaluar su situación y emplear cognición para avanzar a nuevos grados de seguridad y capacidades. Existe la necesidad de que los datos evalúen y configuren su entorno antes de que se abran, analicen comportamientos, realicen análisis de relaciones de datos con datos y emprendan las medidas necesarias para la autoprotección, autodestrucción y, en determinadas circunstancias, informen de vuelta a su creador. Si los propios datos saben quiénes son, en dónde están y cómo deberían interaccionar, estos pueden configurar y supervisar el entorno informático para soportar sus propias necesidades. Existe una fuerte necesidad de datos que posean cognición y este nivel de seguridad. Los datos capaces de "pensar por sí mismos" y razonar basándose en su situación podrían hacer avanzar en gran medida la seguridad de datos y volverse un obstáculo importante para la ciberdelincuencia y el ciberterrorismo. El documento WO0125870A2 es parte de la técnica anterior.

Sumario de la invención

[0010] En consecuencia, un objeto de la presente invención consiste en proporcionar un sistema y método para que los datos cognitivos tomen decisiones de forma autónoma y no dependan de recursos de red, Internet o servidores para analizar y controlar el entorno en el que residen los mismos, con lo que los datos se autoprotegen, se autogestionan y, si es necesario, alertan al creador de datos y se autodestruyen.

[0011] Otro objeto de la presente invención es proporcionar seguridad de datos autónoma, cortando la dependencia de soluciones centradas en la red, la administración de sistemas, la gestión de redes y el creador para asegurar que el entorno está libre de condiciones inseguras antes de acceder a los datos. Incrustar seguridad autónoma en los propios datos mitiga las potenciales incidencias de seguridad y errores humanos.

[0012] Otro objeto de la presente invención es proporcionar un método y sistema para limitar la exposición del creador a vulneraciones de datos no deseables y actividades cibernéticas maliciosas que impliquen robo o medios poco escrupulosos de obtención de datos implementando un nuevo medio de seguridad de procesamiento de datos en donde puede incrustarse seguridad autónoma en datos que comprenden documentos digitales, bases de datos digitales, archivos de datos digitales, medios digitales y multimedios digitales.

[0013] Otro objeto de la presente invención es proporcionar un método y sistema en donde solo existan instanciaciones de datos de las que el creador sea consciente. Por lo tanto, el creador conserva control de sus datos.

[0014] Otro objeto de la presente invención es retirar el acceso directo a datos altamente sensibles mediante la sustitución de campos de etiqueta significativos, quitando de este modo los datos altamente sensibles para proteger los mismos adicionalmente frente a vulneraciones y manipulación errónea.

[0015] Otro objeto de la presente invención es proporcionar un método y sistema para el comportamiento de interrelaciones de datos con datos en donde estos datos pueden analizar y razonar entre sí posibilitando análisis, cálculos y evaluaciones, realizando de este modo análisis situacionales inteligentes, haciendo determinaciones condicionales y presentando conclusiones de datos de orden superior.

[0016] Otro objeto de la presente invención es crear un motor de cognición que posibilite un fundamento para la inteligencia, la adaptabilidad y el razonamiento de datos.

[0017] Otro objeto de la presente invención es proporcionar un método y sistema en donde se alerta al creador de una situación urgente o de emergencia en donde sus datos están comprometidos y/o se han obtenido de forma maliciosa. Esta alerta podría resolver infracciones graves posibilitando que el creador responda inmediatamente para proteger su privacidad frente a situaciones tales como robo de identidad a través de la apropiación indebida de datos.

[0018] Un objeto más de la invención es proporcionar una metodología y sistema en el que datos se autogestionan y se autocontrolan dependiendo del nivel de seguridad que necesiten los datos, las evaluaciones de comportamiento que realizan los datos, la hora del día, la frecuencia con la que se accede, la edad, la duración de acceso, el nivel de seguridad y/o sensibilidad y atributos de campo de datos de los datos particulares creados de acuerdo con las preferencias de creador.

[0019] En una forma de realización de la presente invención, un método y sistema protege ventajosamente la exposición del usuario a actividad no deseada y maliciosa empleando mecanismos de control avanzados implementados como una capacidad de procesamiento de datos incrustada. La metodología y sistema de datos cognitivos permite que el creador tome proactivamente el control de quién, cómo, cuándo y si otra parte puede poseer sus datos. Ventajosamente, la metodología divulgada transforma datos desde un archivo pasivo que puede ser obtenido, comprometido y usado indebidamente por cualquiera a una instanciación de datos cognitivos que posee control de entorno y autogestión ofreciendo al creador protección, seguridad y análisis avanzados. Tras asociar el creador palabras clave, aspectos clave y/o elementos clave del cuerpo de datos con etiquetas y/o funciones, éstos pueden aprovecharse para realizar análisis. Esta capacidad puede personalizar datos cognitivos según las prioridades y necesidades del creador para mantener privados los datos sensibles. También proporciona medios inteligentes para una configuración singular del entorno basándose en requisitos de seguridad de datos, para autoproteger mientras está en uso. Los datos cognitivos se gestionan y se controlan dependiendo del entorno, el estado, la seguridad, la confianza y el nivel de inteligencia de la instanciación de datos cognitivos particular. Los datos pueden realizar análisis de comportamiento para soportar sus necesidades y las de su creador o usuario. Se capacita al creador para tomar el control sobre y limitar el acceso a sus datos sensibles privados. También se implementa inteligencia artificial para crear una capacidad de cognición de datos adaptativa.

[0020] Se divulga un método y sistema para la creación y el procesamiento de datos cognitivos. En una forma de realización, el sistema es un marco que comprende un motor de cognición, una estructura de datos cognitivos y procesos de soporte en un entorno computacional tal como un ordenador. Las preferencias de creador se seleccionan de entre una pluralidad de niveles de cognición y seguridad, controles de acceso y gestión de datos y permisos tras la creación de datos cognitivos. Se usa un quitador de datos para extraer y cifrar datos altamente sensibles que pueden representarse con etiquetas de campo de datos asociadas. Las etiquetas de campos de datos asociadas y otras características de datos pueden aprovecharse para realizar análisis de evaluación y comportamiento de datos con datos. El método incluye supervisar el entorno computacional para detectar un cambio de estado en una instanciación de datos cognitivos, determinar quién creó originalmente los datos, si el usuario actual es el creador y si se permite al usuario poseer la instanciación de datos cognitivos. Si se permite la instanciación, se determinan los requisitos de seguridad. Entonces, el entorno se configura en consecuencia, concediendo por último al usuario actual acceso a los datos dependiendo de los controles y limitaciones del creador. Si no se permite la instanciación, los datos cognitivos realizan un autoanálisis y una autogestión que comprende el nivel de inseguridad, el análisis de comportamiento, el análisis de datos con datos y la autodestrucción de los datos. Cuando los datos cognitivos detectan una apropiación indebida, alertan al creador comprendiendo la identidad del delincuente y su entorno posibilitando al creador un control remoto de los datos cognitivos incluso después de una situación de vulneración. La invención es como se define en las reivindicaciones adjuntas.

Breve descripción de los dibujos

[0021] Las características de la invención que se creen novedosas se exponen específicamente en las reivindicaciones adjuntas. Sin embargo, la invención propiamente dicha, tanto en cuanto a su estructura como a su método de funcionamiento, puede entenderse mejor haciendo referencia a la siguiente descripción y a los dibujos adjuntos.

La figura 1 es un diagrama de bloques funcionales que muestra la relación global del sistema y el método de datos cognitivos divulgado en relación con entornos en los que reside este.
La figura 2 es un diagrama de bloques funcionales que muestra los elementos básicos del marco de datos cognitivos.
La figura 3 es un diagrama de flujo del proceso de nivel de seguridad de procesador de datos cognitivos.
La figura 4 es un diagrama de flujo del proceso de nivel de inteligencia de procesador de datos cognitivos.
La figura 5 es el diagrama de flujo del proceso de acceso a datos de procesador de datos cognitivos.
Las figuras 6 y 7 son los diagramas de flujo para el proceso de estructura de datos.
La figura 8 es el diagrama de flujo del proceso quitador de datos.
La figura 9 es el diagrama de flujo del proceso de entorno de la instanciación de datos cognitivos actual.
La figura 10 representa el diagrama de bloques funcionales de agente inteligente mostrando los componentes globales de una estructura de agente inteligente sencilla.
La figura 11 es un diagrama de bloques del sistema de múltiples agentes de datos cognitivos que representa los componentes y sus relaciones.
La figura 12 es el diagrama de flujo del agente inteligente observador.
La figura 13 es el diagrama de flujo del agente inteligente aprobador para el precepto de agente observador.
La figura 14 es el diagrama de flujo del agente inteligente aprobador de creador para el precepto de agente delator.
La figura 15 es el diagrama de flujo para el agente inteligente delator del precepto de aprobador.
La figura 16 es el diagrama de flujo para el agente inteligente delator del precepto de salud.
La figura 17 es el diagrama de flujo para el agente inteligente de salud de los preceptos de agente delator, agente aprobador y agente rastreador.
La figura 18 es el diagrama de flujo para el agente inteligente rastreador del precepto de observador.
La figura 19 es el diagrama de flujo para el diagrama de flujo de agente inteligente de comportamiento para la

ubicación de empresa.
La figura 20 es la representación gráfica de las funciones de pertenencia de horario de trabajo.
La figura 21 es la representación gráfica de las funciones de pertenencia de entorno remoto.
La figura 22 es la representación gráfica de las funciones de pertenencia de uso de historia.
La figura 23 es el diagrama de flujo del procesamiento de inferencia difusa.
La figura 24 es un diagrama de bloques de recursos de hardware necesarios para soportar el sistema y método de datos cognitivos divulgado. La implementación del hardware puede ser o bien una unidad autónoma que interactúa con funciones externas del dispositivo o un elemento/conjunto de características integrado.

Descripción detallada de la invención

[0022] La presente invención incluye un sistema y método de datos cognitivos que posibilita que el creador de datos sensibles y privados mantenga el control incluso después de una vulneración intrusiva y una actividad maliciosa. Esta invención ofrece privacidad de datos, seguridad y protección al creador. Ventajosamente, los sistemas y métodos de la presente invención posibilitan a los consumidores recuperar el control de sus datos almacenados digitalmente, logrando privacidad y seguridad de datos autónoma a un nuevo nivel incrustando estas capacidades habilitantes. Junto con estas ventajas, el creador de los datos puede incrustar preferencias proactivas para la gestión de datos y ser alertado de que otra parte adquiera sus datos y del estado de dichos datos. El creador puede indicar si dichos datos deberían autodestruirse, eliminando de este modo la instanciación de los datos objeto de apropiación indebida. Esta capacidad posibilita que el creador mantenga el control remoto de sus datos. Esta invención proporciona a los usuarios medios retroactivos tras el evento de una vulneración de datos o ciberataque.

[0023] Solo para fines de ilustración, y para no limitar la generalidad, el sistema y método de datos cognitivos se explicará con referencia a su uso en un entorno informático digital. Las expresiones datos cognitivos y datos inteligentes son equivalentes y pueden intercambiarse en el presente documento. Los estados, el marco, la creación, la gestión de datos y entornos y el procesamiento de datos cognitivos comprenden un ejemplo de esta aplicación. El sistema y método de datos cognitivos incluye una lógica de control automatizada que integra de forma inteligente las funciones de control y gestión de datos, brindando un sistema proactivo con preferencias de control de usuario y cognición de datos incrustadas. Este sistema y método de datos cognitivos posee datos que pueden estar en uno de al menos tres estados:

- **Estado activo o "atento"** en donde los datos se están usando, creando, manipulando, abriendo, modificando, copiando, etc.
- **Estado latente o "en reposo"** en donde los datos no están en uso (por ejemplo, los datos están almacenados en medios digitales).
- **Estado en movimiento** en donde está teniendo lugar la transmisión de los datos. El estado en movimiento puede considerarse un tipo de estado "atento" debido a que los datos cognitivos son conscientes de este evento.

[0024] El sistema y método de datos cognitivos puede existir en una pluralidad de entornos o dominios. Más particularmente, la figura 1 es un diagrama de bloques funcionales que muestra la relación global del sistema 100 y método de datos cognitivos divulgado en relación con entornos o dominios en los que pueden residir y funcionar los datos cognitivos. Los datos pueden existir en un entorno de creador 101, que es el entorno del que proceden los datos (es decir, la instanciación original). Los datos también pueden residir en el entorno de red 102 (por ejemplo, un servidor de red o Internet). Los datos pueden residir en un entorno de almacenamiento 103 (por ejemplo, medios de almacenamiento, discos duros, DVD, CD-ROM, unidades de disco, memorias USB, etc.). Puede accederse a este entorno de almacenamiento 103 o bien a través del entorno de creador 101 directamente (es decir, la comunicación de puerto de dispositivo de medios con el puerto de entorno de creador a través de hardware o de forma inalámbrica) o bien indirectamente a través de un entorno de red 102 (por ejemplo, un servidor de red local o residiendo de forma remota a través de recursos de Internet). Por último, los datos pueden residir en el entorno 104 de una parte de recepción tal como un ordenador de la parte de recepción. Los datos pueden recibirse en el entorno de receptor 104 a través de unos medios de un entorno de almacenamiento 103 o a través de unos medios de un entorno de red 102.

[0025] En la figura 2 se representa un marco de datos cognitivos 200. Este marco 200 comprende un procesador de datos cognitivos 201 que posibilita el procesamiento, creación, cognición y control global de datos cognitivos. El marco de datos cognitivos 200 comprende también un procesador de entorno 202 para configurar, asegurar y controlar recursos de entorno tras un cambio de "estado" de los datos cognitivos. El procesador de entorno 202 configura y controla los puertos, dispositivos, recursos y procesos 203. Las preferencias de creador y los recursos necesarios para crear, soportar y procesar datos cognitivos se proporcionan y se almacenan en los recursos y repositorio de memoria de datos cognitivos 204 del entorno. El procesador de datos cognitivos 201 accede al procesador de estructura de datos 205 para crear y acceder a datos cognitivos.

[0026] Como un ejemplo de procesamiento funcional, supóngase que un usuario de un entorno decide acceder a Internet mientras está activo un archivo de datos cognitivos de nivel de seguridad alto; el procesador de entorno 202 cerraría entonces el archivo de datos cognitivos de seguridad alta, abriría los puertos y activaría los procesos 203 necesarios para que el usuario acceda a Internet. A la inversa, estos puertos se cerrarían para reabrir el archivo de datos cognitivos. Adicionalmente, los recursos y repositorio de datos cognitivos 204 pueden comprender información

de registro, instanciaciones de agentes inteligentes (AI) que van a usarse y/o asociarse con datos cognitivos, datos quitados (es decir, elementos de datos o campos extraídos o quitados del cuerpo principal de un archivo de datos cognitivos), y metadatos adicionales. El acceso a los recursos y repositorio de datos cognitivos 204 puede restringirse para proporcionar protección adicional para asegurar los contenidos.

[0027] Los componentes del procesador de datos cognitivos 201 en esta realización comprenden un proceso de nivel de seguridad, un proceso de nivel de inteligencia, un proceso de acceso, un proceso de estructura de datos, un proceso quitador, un proceso de entorno, y un motor de cognición producido por un sistema de múltiples agentes (MAS). El motor de cognición se incorpora al archivo de datos cognitivos. Se incorpora una estructura de datos exhaustiva a este procesamiento. Esta forma de realización produce un conjunto de datos cognitivos en donde se produce un archivo de datos cognitivos junto con un archivo de datos cognitivos quitados asociado que contiene información altamente sensible.

[0028] Un examen adicional de los datos cognitivos en lo que se refiere a la gestión de autoprotección requiere conocimientos de nivel de seguridad. La figura 3 muestra el procesador de datos cognitivos 200 para el flujo de procesamiento de nivel de seguridad. Puede implementarse y soportarse una pluralidad de niveles de seguridad. A modo de ejemplo, esta forma de realización obtiene un ajuste de nivel de seguridad a partir del creador de datos cognitivos a través de entradas de un teclado y/o ratón en un ordenador digital, en donde el procesador de datos cognitivos 200 lee el ajuste de nivel de seguridad de usuario 300 deseado a partir de una pluralidad de configuraciones que comprenden posibilidades de selección de nivel de seguridad bajo 301, medio 302 y alto 303. Entonces, se llama al procesador de entorno en la etapa 304, debido a que la selección de nivel de seguridad influye en los ajustes de entorno requeridos para acceder a y activar los datos cognitivos. Por ejemplo, el ajuste de nivel de seguridad medio 302 puede requerir que el entorno cierre puertos a Internet mientras el archivo de datos cognitivos está en el estado "activo".

[0029] A modo de ejemplo para esta realización, el nivel de seguridad medio 302 incorporará los ajustes de entorno para el nivel de seguridad bajo 301 así como cifrará los datos resultantes. El cifrado puede lograrse a través de software normalizado disponible en el mercado y/o llamadas a sistema operativo. Por ejemplo, la interfaz de programación de aplicaciones de protección de datos (DPAPI) del sistema operativo Windows de Microsoft consiste en un par de llamadas de función que proporcionan protección de datos de nivel de sistema operativo a través de cifrado de datos. Debido a que la protección de datos es parte del sistema operativo, asegurar los datos puede lograrse sin necesidad de ningún código criptográfico específico, aparte de las llamadas de función a DPAPI. Cryptprotect_Promptstruct es la "estructura de aviso" y la estructura de datos protegidos contiene los datos protegidos. Las dos funciones comprenden la función de protección de datos CryptProtectData() y la función de desprotección de CryptUnprotectData().

[0030] En este ejemplo, la selección de nivel de seguridad alto 303 incorpora todos los medios de seguridad del nivel medio 302 de seguridad, así como quita los datos (la acción de quitar datos se analizará más adelante). La selección de nivel de seguridad se usa como una entrada en el procesador de entorno 304 que configura el entorno con el nivel de protección apropiado. Una vez que el procesador de entorno se ha invocado y ha vuelto, este proceso finaliza 305.

[0031] El procesador de datos cognitivos 201 también proporciona medios para que el creador seleccione "cómo de inteligentes" deberían ser los datos cognitivos. La figura 4 representa el flujo de procesamiento de nivel de inteligencia del procesador de datos cognitivos 200. Puede implementarse una pluralidad de niveles de inteligencia. A modo de ejemplo, esta forma de realización obtiene un ajuste de nivel de inteligencia a partir del creador de datos cognitivos a través de entradas de un teclado y/o ratón en donde el procesador de datos cognitivos 201 lee el ajuste de nivel de inteligencia de datos 400 seleccionado por el creador que varía entre "algo inteligente" 401, "inteligente" 402 y "muy inteligente" 403. Para el caso de "algo inteligente" 401, los datos cognitivos se crean 404 aprovechando recursos a partir de los recursos y repositorio de datos cognitivos 204 (la estructura de datos inteligente se define más adelante). Si se selecciona el nivel de inteligencia "inteligente" 402, se crea una creación más cognitiva de la estructura de datos cognitivos (por ejemplo, se usan campos de datos adicionales a los del caso de "algo inteligente"). Y por último, si el creador selecciona el nivel de inteligencia "muy inteligente" 403, se crea la máxima inteligencia que puede alcanzarse (es decir, se incluyen todos los campos de estructura de datos inteligente). Una vez que se ha creado la estructura de datos cognitivos en la etapa 404, este proceso finaliza 405.

[0032] El procesador de datos cognitivos 202 también usa un proceso de acceso que proporciona "acceso a" y/o "creación de" datos cognitivos. La figura 5 representa un diagrama de flujo del proceso de acceso al procesador de datos cognitivos 202. Este proceso comienza tras llamarse desde el MAS del procesador de datos cognitivos 202 (el MAS se analizará más adelante), solicitando acceso de usuario a los datos cognitivos y pasando el argumento de "tipo_solicitud_usuario" en la etapa 500. Se llama al procesador de estructura de datos en la etapa 501 para crear y/o acceder a los datos cognitivos. Se llama al proceso de nivel de inteligencia 502 y se lee el campo de nivel de inteligencia 503. Entonces se llama al proceso de nivel de seguridad 504 para obtener el nivel de seguridad 505 requerido para acceder a o crear los datos cognitivos que posteriormente llaman al procesador de entorno para configurar el entorno informático para satisfacer las necesidades del nivel de seguridad leído a partir de la estructura de datos. Ahora el proceso de acceso está listo para ejecutar el tipo_solicitud_usuario en la etapa 507 dependiendo de los controles, configuración y parámetros de los procesos anteriores y vuelve al proceso de llamada 508.

[0033] El procesador de estructura de datos 205 se basa en el contenido y la estructura del archivo o registro de datos cognitivos. Principalmente, el archivo de datos cognitivos o la estructura de registro de datos cognitivos a modo de ejemplo en esta forma de realización comprende los siguientes campos, metadatos y elementos. Puede lograrse una cognición de datos mayor tras aprovechar los campos de datos adicionales para los casos de "muy inteligente" e "inteligente" más allá de los campos de datos de "algo inteligente". Los campos que se marcan con "(vs)" se incluyen en la estructura de datos de nivel de inteligencia "muy inteligente"; los campos marcados con "(s)" se incluyen en la estructura de datos de nivel de inteligencia "inteligente"; y los campos marcados con "(ss)" se incluyen en la estructura de datos de nivel de inteligencia "algo inteligente" en donde un subconjunto de estos campos de datos comprende una estructura de datos menos cognitivos:

1. Información de encabezamiento / identificador [(vs) (s) (ss) para todos los campos]

- Nombre
- Tamaño
- Tipo
- Aplicación(es) asociada(s) con los datos
- Indicación de tiempo
- Modificado con fecha

2. Identidad de sistema de entorno [(vs) (s) (ss) para todos los campos]

A. (obtenido a partir del comando ipconfig /all)

- Nombre de anfitrión
- Direcciones de servidor(es) de sistema de nombres de dominio (DNS)
- Sufijo de DNS primario
- Tipo de nodo
- Encaminamiento de protocolo de Internet (IP) habilitado
- Apoderado del servicio de nombres de Internet de Windows (WINS) habilitado
- Dirección física
- Protocolo de configuración de anfitrión dinámica (DHCP) habilitado
- Configuración automática habilitada
- Dirección de IP
- Dirección de máscara de subred
- Dirección de pasarela por defecto
- Dirección de servidor de DHCP
- Sufijo de DNS específico de conexión y descripción

B. Adicional [Campos (vs) (s)]

- Uso de certificado digital, licencia y/o identificadores de firma digital
- Uso de datos de inscripción
- Uso de declaraciones o testigos (con entornos .NET)

3. Identidad de creador (además de usar los identificadores de entorno)
(solo la primera instancia de creación de datos cognitivos)

- Nombre [(vs) (s) (ss)]
- Clave de licencia si se usa autenticación [(vs) (s) (ss)]
- Datos de inscripción / autenticación [(vs) (s) (ss)]
- Datos de configuración; una instantánea del entorno para su uso para fines de comparación en procesamientos futuros para ayudar a la verificación de identificación adicional del creador [(vs)]

4. Identidad de usuario [(vs) (s) (ss)]

- Nombre [(vs) (s) (ss)]
- Clave de licencia si se usa autenticación [(vs) (s) (ss)]
- Datos de inscripción / autenticación [(vs) (s) (ss)]
- Datos de configuración; una instantánea del entorno para su uso para fines de comparación en procesamientos futuros para ayudar a la verificación de identificación adicional del usuario [(vs)]

5. Ajuste de nivel de seguridad

- Alto: Cifrar y quitar [(vs) (s) (ss)]
- Medio: Cifrar [(vs) (s) (ss)]

- Bajo:

    - Sin acceso a Internet [(ss)] o,
    - Acceso a Internet limitado [(vs) y (s)] en donde pueden permitirse sitios de confianza

6. Valor de CONFIANZA actual (0, 5, 10) en este ejemplo [(vs) (s) (ss)]

7. Ajustes admisibles de restricciones de recursos o solicitudes de usuario (también puede depender del ajuste del nivel de seguridad; cuanto más alto sea el nivel de seguridad, mayores serán las restricciones y/o los ajustes/preferencias de usuario).

- Restringir copiar (sí/no) [(vs) (s)]
- Restringir imprimir (sí/no) [(vs) (s)]
- Restringir editar (sí/no) [(vs) (s)]
- Restringir borrar (sí/no) [(vs) (s)]
- Restringir guardar (sí/no) [(vs) (s)]
- Restringir visualizar (sí/no) [(vs) (s)]
- Restringir mover (sí/no) [(vs) (s) (ss)]
- Restringir analizar (sí/no) [(vs)]

8. Ajustes de control de entorno como una función del nivel de seguridad

- Estado de red (por ejemplo, usando el comando de sistema operativo "netstat -a" que devuelve información con respecto a cualquier otro que esté conectado a su entorno a través de cualquier puerto así como proporciona una lista de todos los puertos abiertos (una potencial entrada remota) en donde cerrar puerto (identidad de puerto) para cada puerto no necesario incluye cerrar puertos remotos (cierre de puertos remotos) [(vs) (s) (ss)]
- Cerrar aplicación de software (nombre de aplicación) para cada aplicación no necesaria [(vs) (s) (ss)]
- Cerrar dispositivo de recursos (identidad de recursos) para cada dispositivo no necesario [(vs)]
- Manipulaciones de archivo admisibles dependiendo del nivel de seguridad [(vs) (s) (ss)]

    - Seguridad alta: Impresión, copia, impresiones de pantalla y modificación de datos autenticadas
    - Seguridad media: Modificación autentificada

9. Control de edad [(vs) (s) para todos los campos]

- Hora y fecha de creación inicial
- Límite de edad o expiración (para cada ajuste de temporizador o una expiración asociada a un evento o a una fecha o duración)
- Actualizar tiempos de guardado
- Tiempo durante el cual está activo
- Hora al día de acceso
- Día de la semana

10. Ajuste de nivel de inteligencia (este campo indica funciones de soporte anexas que posibilitan la inteligencia) [(vs) (s) (ss) para todos los campos]

11. Quitador [(vs) (s) (ss) para todos los campos]

- Identidad de quitador
- Atributos de quitador
- Codificación de quitador

12. Etiqueta asociada [(vs) (s) (ss) para todos los campos]

- Etiqueta de identidad de quitador
- Etiqueta de atributos de quitador
- Etiqueta de codificación de quitador

13. Nombres de datos relacionados [(vs)]

- Este campo permite que el usuario asocie otros archivos de datos a éste.

14. El cuerpo [(vs) (s) (ss) para todos los campos]

- El registro de contenido real que se está creando (también puede ser una base de datos o tablas, medios,

multimedia, etc.)
(Cifrado si el nivel de seguridad es mayor que "bajo")

15. Descargo de responsabilidad [(vs) (s) (ss) para todos los campos]

□ Declaración con respecto a que el archivo de datos creado tiene permiso limitado de su existencia en donde su existencia puede ser controlada por el creador.

[0034] Obsérvese que el "creador" se identifica de forma singular en la primera instanciación de la creación de datos cognitivos. Todas las otras instanciaciones comprueban la identidad del "usuario actual" para determinar si el creador original es el usuario actual. Esta distinción es necesaria para dar al creador original control de sus datos cognitivos incluso desde un entorno remoto. También debería hacerse notar que un registro es creado por unos medios de seguimiento de eventos (es decir, el agente rastreador que se analizará más adelante). Estos datos de registro están compuestos por todos los campos de estructura de datos excepto el cuerpo. Estos campos proporcionan trazabilidad de los datos cognitivos.

[0035] El archivo de datos cognitivos o conjunto de registros de datos cognitivos se implementa como un "documento inteligente", "documento inteligente" es una expresión general para describir documentos electrónicos con más funcionalidad que una página diseñada para emular papel. Por ejemplo, el PDF de Adobe, InfoPath de Microsoft, Cardiff Software y XForms del W3C, y las soluciones no programáticas AjlDocs e Intelledox son documentos inteligentes y se basan en el uso de XML como un formato para datos. Los documentos inteligentes son, en esencia, documentos electrónicos interactivos. Esta capacidad se usa para posibilitar que los datos cognitivos respondan a diversos cambios de estado y eventos, así como para interaccionar con otros procesos divulgados en el presente documento.

[0036] Para proceder, se introduce un parámetro de "confianza". La "confianza" es un parámetro o medida de certeza relativa en donde una "confianza" aumentada infiere un calificador de seguridad. A la inversa, el parámetro "confianza" puede disminuirse para inferir el riesgo. La cognición adicional del comportamiento de usuario implementada, de acuerdo con la presente invención, puede aumentar y disminuir el parámetro "confianza" en consecuencia. Se establece un grado de confianza en donde un grado de confianza alto puede indicarse con un número relativamente alto, y un grado de confianza bajo puede indicarse con un número relativamente bajo. Aunque el ejemplo siguiente indica la confianza usando un grado de confianza numérico, por supuesto también pueden usarse otros métodos para indicar la confianza, tales como indicar la confianza usando información textual, palabras clave u otros indicadores. La implementación de "confianza" en un ejemplo comprende una escala de 0 a 10 con las siguientes indicaciones discretas:

- "Confianza" igual a diez indica que la instanciación del conjunto de datos cognitivos es nueva (es decir, la primera instanciación del archivo de datos cognitivos) y "de confianza" lo que infiere que hay una instanciación existente en el entorno del creador o que el creador ha concedido permiso para la existencia de la instanciación.
- "Confianza" igual a cinco indica que la instanciación no reside en el entorno de creador.
- "Confianza" igual a cero indica desconfianza, una instancia en donde una instanciación del conjunto de datos cognitivos es inaceptable.

[0037] El procesador de estructura de datos 205 crea nuevos datos cognitivos y activa datos cognitivos existentes. Las figuras 6 y 7 representan el diagrama de flujo del proceso de estructura de datos 205. Este proceso comienza con la lectura de los campos de registro de datos de encabezamiento e identificador en la etapa 600. Obsérvese que no hay datos presentes si este es un nuevo archivo de datos cognitivos (es decir, antes de que el creador guardara o escribiera inicialmente los medios en la memoria del entorno). Si los datos acaban de crearse (es decir, no se han guardado antes) 601, entonces se crea el registro de estructura de datos 602, la "confianza" se establece a diez en la etapa 605 y el entorno actual se establece al entorno de creador en la etapa 606. Para el caso de un archivo de datos cognitivos preexistente en la etapa 601, los datos de entorno se comparan con los campos de datos prerregistrados en la etapa 603 para determinar si el entorno es el mismo. Si se determina que el entorno es el mismo en la etapa 604, la "confianza" se establece a diez en la etapa 605 y el entorno actual se establece al entorno de creador en la etapa 606. Si se determina que el entorno no es el entorno de creador en la etapa 604, entonces esta es una instanciación de un archivo de datos cognitivos existente en un entorno de no creador y en la etapa 608 se usará el valor de confianza a partir del registro almacenado. Una vez que se ha establecido el entorno y la identidad de usuario/creador, se realiza la autenticación del usuario usando medios tales como contraseñas de acceso de usuario en la etapa 607. Entonces, se realiza una comprobación en la etapa 609 para determinar si el nivel de seguridad es "alto". Si el nivel de seguridad es "alto", se llama al proceso quitador en la etapa 610 para acceder a unos datos cognitivos asociados altamente sensibles y validar adicionalmente al usuario/creador.

[0038] El procesamiento continúa en la figura 7 en donde se lee el nivel de inteligencia en la etapa 700 (desde el proceso de entrada anterior 400). El procesamiento para una pluralidad de niveles de inteligencia comienza con una comprobación en la etapa 701 para determinar si el nivel de inteligencia es "muy inteligente". Si el nivel de inteligencia es "muy inteligente", entonces se aplican los recursos y los campos de estructura de datos predeterminados para esta condición para producir el registro de datos cognitivos en la etapa 702. Si el nivel de inteligencia es "inteligente", como

se determina en la etapa 703, entonces se aplican los recursos y campos de estructura de datos predeterminados para esta condición para producir el registro de datos cognitivos en la etapa 704. Para los casos de "muy inteligente" e "inteligente", se establecen restricciones de uso en la etapa 706 y se obtienen controles de tiempo/evento o bien a partir de los datos almacenados o bien a partir del usuario/creador en la etapa 707. Estas preferencias de restricción de entrada se usan para gestionar y limitar el uso futuro de la instanciación de datos resultante. Y por último, si el nivel de inteligencia no es "muy inteligente" o "inteligente", entonces se usan recursos y campos de estructura de datos "algo inteligentes" en la etapa 705.

[0039] Los recursos de nivel cognitivo comprenden funcionalidades adicionales que incorporan "¿cómo de inteligentes tienen que ser los datos?". Por ejemplo, si el creador necesita que el conjunto de archivos de datos cognitivos exista solo durante una respuesta a un incidente de emergencia en donde los datos se comparten entre agencias gubernamentales para soportar la interoperabilidad, este archivo de datos podría restringirse para autodestruirse (es decir, borrar la instanciación del conjunto de datos) tras el final de la sesión de comunicación interoperable en la que se usa. Otro ejemplo puede comprender un tiempo de expiración tras el cual el archivo de datos se autodestruirá o un tiempo de archivo en donde los datos se autoarchivarán automáticamente. El autoarchivado podría referirse a que el archivo de datos cognitivos se comprimiera a sí mismo y se moviera a una ubicación de archivo de memoria específica que podría ser memoria en el repositorio de datos cognitivos 204.

[0040] Comenzando con la etapa de "establecer restricciones de uso" en la etapa 706, el proceso comprende que el creador indique las limitaciones de manipulación de archivos de datos resultantes, tales como limitar el número de veces que puede abrirse un archivo de datos cognitivos, inhibir la modificación (por ejemplo, el usuario posterior no puede editar los datos cognitivos) o establecer el tiempo durante el cual puede visualizarse un archivo de datos en cualquier momento. El procesamiento continúa para obtener los controles y accesos de recursos de entorno en la etapa 708 dependiendo de niveles de seguridad e inteligencia que van a emplearse. Entonces, en la etapa 709, el conjunto de registros de datos cognitivos y los recursos asociados se escriben en la memoria y el proceso vuelve al procedimiento de llamada en la etapa 710.

[0041] En esta forma de realización, el nivel de seguridad "alto" requiere el uso de quitar datos altamente sensibles de los datos del documento y almacenar los mismos en un archivo de datos cognitivos separado. Las muestras de datos altamente sensibles podrían comprender números de identidad tales como números de seguridad social, nombres, ubicaciones, números financieros, información de precios, etc. En la figura 8 se representa el diagrama de flujo del proceso quitador. Tras un evento de llamada en la etapa 800, se hace una comprobación para determinar si el archivo de datos ya existe o si se está creando un nuevo archivo de datos en la etapa 801. Si el archivo de datos es preexistente, entonces se realiza otro proceso de autenticación de usuario en la etapa 802 antes de abrir el archivo de datos quitados en la etapa 803 para añadir otra capa de seguridad. Si los datos son nuevos en la etapa 801, entonces este proceso obtiene las entradas de palabras clave a partir del creador a través del teclado y/o ratón en la etapa 804 y escribe dichas palabras clave y sus etiquetas asociadas en matrices separadas en la etapa 805 para almacenar las mismas en una memoria separada. Este proceso se repite hasta que todas las palabras clave y sus etiquetas asociadas han sido introducidas en la matriz por las etapas 805, 806. Una vez se ha completado, se crea el registro de datos cognitivos para las palabras clave quitadas y otro registro de datos cognitivos para las etiquetas asociadas en la etapa 807. Entonces, los nombres de los datos relacionados se registran en la etapa 810 (los nombres de los datos relacionados se analizarán más adelante), y el procesamiento finaliza en la etapa 808.

[0042] El proceso quitador incorpora un campo adicional para que lo utilice el creador denominado etiqueta asociada. Como ejemplo de la etiqueta asociada, considérese la instancia en donde el creador selecciona "000-000-000AA", su número de cuenta bancaria, para que se le quiten datos cognitivos que se están creando. Junto con esto, el creador asocia el campo de texto: "mi número de cuenta bancaria" como la etiqueta asociada.

[0043] El uso de esta interrelación de datos con datos permite que el creador alcance otro orden de seguridad para datos altamente sensibles. Por lo tanto, cuando se visualiza el documento final en este ejemplo, aparecería el "número de mi cuenta bancaria" en lugar de "000-000-000AA" en el documento resultante. Además, la capacidad de asociación de datos con datos puede posibilitar un procesamiento avanzado.

[0044] El flujo de proceso para los campos de "Nombres de datos relacionados" puede soportarse con un proceso que solicite al creador o usuario que facilite los nombres de otros archivos de datos que desee asociar con el archivo de datos cognitivos actual, de haber alguno. Esta lógica también puede usarse para "marcar" palabras clave en el cuerpo o contexto de la estructura de archivo de datos. Esta utilidad puede usarse para realizar análisis de datos con datos avanzados. A modo de ejemplo, si una instanciación de datos cognitivos contiene campos financieros de los ingresos del día anterior de una pequeña empresa, si el archivo de datos cognitivos actual está asociado a este archivo de datos anterior, se podrían habilitar unos análisis que calculen y deriven conclusiones financieras.

[0045] Es necesario controlar el entorno para proteger los datos. Para ello se usa el diagrama de flujo del proceso de entorno 202 representado en la figura 9. El proceso de entorno 202 es responsable de configurar el entorno para proteger los datos cognitivos. Los controles y ajustes de entorno dependen del nivel de seguridad requerido mientras los datos cognitivos están en el estado "activo". Este proceso comienza en la etapa 900 obteniendo el nivel de seguridad a partir del procesador de datos cognitivos 201. Si el nivel de seguridad es "alto" en la etapa 901, entonces

se invocan las condiciones de restricción de entorno "alta" en la etapa 905. Las restricciones a recursos innecesarios son las mayores para este nivel de seguridad. El nivel de seguridad "alto" en este ejemplo comprende:

- Cerrar todos los puertos no esenciales (permitir solo que permanezcan abiertos puertos esenciales tales como el teclado, el ratón y el puerto de vídeo del monitor).
- Cerrar procesos activos innecesarios en el entorno; cerrar procesos que se activan pero que no son necesarios para la creación y el procesamiento de los datos cognitivos. Por ejemplo, un proceso de actualización de Microsoft, un correo electrónico o un proceso de barra de herramientas de Google puede estar activo y procesándose en la memoria de acceso aleatorio (RAM), pero no es necesario para la creación y manipulación de datos cognitivos, por lo que estos procesos no esenciales se terminan si los datos son "muy inteligentes".
- Puede ser necesario que haya disponibles recursos tales como una impresora o una base de datos para soportar la creación del archivo de datos cognitivos y éstos pueden ser seleccionables por el usuario a través de una interfaz de usuario de tal modo que los medios para acceder a dichos recursos y/o dispositivos podrían permitirse de una forma limitada dependiendo de la selección del creador.

[0046] Si el nivel de seguridad es "medio" en la etapa 902, entonces se usan las restricciones de entorno "medias" en la etapa 903. El nivel "medio" no está tan restringido como el nivel "alto". Puede permitirse la ejecución de más procesos en segundo plano (por ejemplo, correo electrónico) y puede haber más accesos a puertos sin necesidad de cerrar en primer lugar el archivo de datos (por ejemplo, acceso a Internet). Por último, si el nivel de seguridad es "bajo" en la etapa 904, entonces, se podría permitir el acceso de control de puertos en donde se podrían configurar ligeras limitaciones de acceso a una conexión a Internet (por ejemplo, solo pueden visitarse sitios "de confianza" mientras los datos cognitivos están en un estado "activo"). Una vez se han determinado restricciones de entorno basándose en el nivel de seguridad, los puertos y accesos (por ejemplo, acceso remoto) del entorno se configuran en consecuencia en la etapa 906. Entonces, en las etapas 907 y 908 se configuran controles de procesos y controles de recursos, respectivamente. El entorno está ahora asegurado para que el usuario/creador pueda acceder a los datos cognitivos "activos" y este proceso finaliza en la etapa 909.

[0047] Obsérvese que pueden incorporarse esquemas tales como "golpeteo de puertos" para proteger adicionalmente el entorno mientras los datos cognitivos están en un estado "activo". El golpeteo de puertos se usa para impedir que un atacante explore un sistema en busca de servicios potencialmente explotables, protegiendo de este modo los puertos para que parezcan cerrados.

[0048] El procesador de datos cognitivos 201 en esta forma de realización se implementa aumentando los procesos descritos previamente con un sistema de múltiples agentes (MAS) que comprende agentes inteligentes (AI). La figura 10 representa elementos fundamentales de un AI sencillo en donde el programa del agente inteligente 1000 es una función que implementa la correlación de agente de los preceptos 1001 a las acciones 1007. Los preceptos de entorno 1001 se alimentan a los sensores 1002 del AI. El estado 1003 es "cómo es el mundo ahora" para el AI. Dado dicho estado 1003 y aplicando las reglas 1005 del AI, brinda las acciones 1004 específicas emprendidas por el AI. En un caso sencillo, hallando una regla 1005 que coincide con la situación actual (como se define en el precepto), realizar la acción 1004 asociada con esa regla 1005 particular. Las acciones 1004 son las entradas a los accionadores 1006 que dan como resultado acciones emprendidas para el entorno 1007 del AI. AI más complejos incluyen agentes de aprendizaje que también pueden emplearse. La arquitectura global del marco de datos cognitivos 200 en esta realización está soportada por una colección de estos agentes especializados o AI. La cognición se realiza como un conjunto de representaciones y modelos que intercambian información entre estos AI y representaciones. Cada unidad funciona como un mecanismo cognitivo para lograr un aspecto particular de la inteligencia, tal como tras la percepción de un evento, seleccionar una(s) acción(es) apropiada(s), etc.

[0049] El MAS para esta invención de datos cognitivos se representa en la figura 11. Un fin primario del MAS es asegurar que el propio archivo de datos cognitivos no se vea comprometido. Este MAS está compuesto por una pluralidad de AI que residen en el registro y/o conjunto de registros de datos cognitivos. El AI observador 1101 supervisa las acciones de entorno 1100 en relación con el acceso y la manipulación de datos cognitivos, el repositorio de datos cognitivos y memoria. El AI rastreador 1102 registra todos los eventos que ocurren con los datos cognitivos. El rastreador también interactúa con el AI de comportamiento 1108. El AI de comportamiento 1108 realiza análisis de comportamiento en donde el análisis de comportamiento puede ser de eventos del entorno, comportamiento de usuario, comportamiento de datos con datos, etc. El AI de salud 1103 determina el "estado de salud" del conjunto de archivos de datos cognitivos y controla la existencia de la instanciación particular de datos cognitivos. El AI delator 1104 recopila información e informa de vuelta al creador de datos cognitivos. El AI delator posibilita que los creadores controlen sus datos incluso en una situación comprometida. El agente observador 1100, el agente rastreador 1101, el agente de comportamiento 1108, el agente de salud 1103 y el agente delator 1104 son AI incrustados que coexisten en el mismo archivo o registro físico que la estructura de datos cognitivos 1105. El AI aprobador 1107 informa al creador y/o usuario. Junto con los informes, este también proporciona los medios para interaccionar con dicho creador y/o usuario para gestionar y controlar los datos cognitivos asociados.

[0050] La figura 12 muestra el diagrama de flujo de proceso de AI observador. El fin primario del AI observador 1101 es supervisar y detectar un cambio en el estado del archivo de datos cognitivos 1106. El estado de datos cognitivos de observador se establece inicialmente a "latente" en la etapa 1200. La supervisión de los medios de entrada de

usuario del entorno informático digital (es decir, los sensores de AI 1002) comienza en la etapa 1201. Los sensores del agente observador comprenden capacidades de entrada/salida tales como el teclado, el ratón, la comunicación de puertos y los comandos de sistema operativo. Los preceptos 1001 a partir del entorno comprenden solicitudes de usuario tales como las siguientes:

- Abrir (estado activo)
- Imprimir (estado en movimiento)
- Editar (estado activo)
- Borrar (estado activo)
- Guardar (estado activo si se vuelve a guardar una nueva instanciación del mismo conjunto de archivos de datos; estado en movimiento si se guarda una instanciación completamente nueva del conjunto de archivos de datos)
- Copiar (estado en movimiento debido a que esta es una instanciación completamente nueva del conjunto de archivos de datos; esto también es representativo de la transmisión, debido a que se crea una nueva instanciación del conjunto de archivos de datos en el entorno de recepción)
- Mover (estado en movimiento)
- Visualizar (estado activo)
- Analizar (estado activo)

[0051] Suponiendo un estado latente inicial y tras la selección del usuario del archivo de datos cognitivos (por ejemplo, "abrir" la selección del archivo de datos cognitivos detectada a través de un "clic" del dispositivo de entrada del ratón), el estado 1003 del archivo de datos cognitivos se detecta como un cambio de estado en la etapa 1202, y el estado se cambia a "activo" en la etapa 1203. La acción 1004 del AI tras volverse "activo" el archivo de datos cognitivos es llamar al AI rastreador en la etapa 1206 (lo que registrará este evento). Es aplicable la siguiente regla 1005:

SI estado = activo ENTONCES llamar a rastreador (estado_actual, solicitud_usuario)

en donde el accionador 1006 llama al AI seguidor en la etapa 1206. Las acciones resultantes para el entorno 1007 comprenden invocar el AI rastreador en la etapa 1206 y pasar los datos de estado_actual y los parámetros de solicitud_usuario como argumentos de proceso. El procesamiento vuelve a la supervisión de un cambio en el estado del archivo de datos cognitivos de la etapa 1202 después de que memoria temporal y registros se hayan limpiado en la etapa 1208. A la inversa, si el cambio de estado detectado es al estado latente en la etapa 1202, entonces el estado del observador 1101 se mantiene como "latente" en la etapa 1204 y el proceso vuelve a supervisar el archivo de datos cognitivos en busca de cambios de estado en la etapa 1201 después de que la memoria temporal y los registros se hayan limpiado en la etapa 1208. Por último, si se ha detectado el cambio de estado 1202 a "en movimiento" en la etapa 1205, entonces se aplica la regla 1005:

SI estado = en movimiento ENTONCES llamar a aprobador (estado_actual, tipo_solicitud_usuario)

en donde el accionador 1006 llama al AI aprobador 1007 en la etapa 1207. Los resultados de esta función proporcionan medios para alertar al usuario de un tipo de solicitud de "mover datos". Tras volver el procesamiento al proceso del agente observador, los recursos de entorno que accedieron a los datos cognitivos necesitan hacer que la memoria temporal se "limpie" o se sobrescriba en la etapa 1208 de tal modo que se almacenan datos altamente sensibles, tales como códigos de acceso y claves, completando de este modo el proceso en la etapa 1209.

[0052] Principalmente, el AI aprobador 1107 realiza comprobaciones de autenticación y aloja aprobaciones de acciones de creador. Los preceptos proceden del delator 1104 y del observador 1101. Los campos del archivo de datos cognitivos o del registro de datos cognitivos, excepto el cuerpo de datos real, comprenden los sensores 1002 (es decir, metadatos) y sus valores constituyen el estado 1003. Las acciones emprendidas dependen de las reglas 1005 que pueden comprender lo siguiente:

SI seguridad aceptable ENTONCES permitir solicitud_usuario
SI seguridad algo aceptable ENTONCES notificar a delator
SI seguridad NO aceptable ENTONCES denegar tipo_solicitud_usuario Y notificar salud

en donde "seguridad aceptable" equivale a que los ajustes de entorno actuales coincidan con o superen el valor de datos de nivel de seguridad en el registro de datos cognitivos y el valor de confianza; "seguridad algo aceptable" depende de la lógica de delator (que va a analizarse más adelante); y "seguridad NO aceptable" equivale a que la identidad de usuario actual no coincida con la identidad de creador y a la ausencia de una sensación de "confianza".

[0053] La figura 13 muestra un diagrama de flujo para explicar mejor el agente aprobador 1107 en lo que se refiere al agente observador 1101 y al precepto 1001. El procesamiento comienza tras recibir una llamada desde el agente observador 1101 en la etapa 1300. En la etapa 1301 se realiza una comprobación para determinar si el usuario actual es el creador del archivo de datos cognitivos comparando los campos de identidad de creador del registro de datos cognitivos con los campos de identidad de usuario actual. Si la identidad de creador es igual a la identidad de usuario, entonces, en la etapa 1302 se realiza una comprobación para determinar si se permite el tipo_solicitud_usuario basándose en los ajustes de campo de registro de datos cognitivos almacenados. Si se permite el

tipo_solicitud_usuario, en la etapa 1310 se llama al proceso de acceso pasando el argumento tipo_solicitud_usuario y el proceso termina en la etapa 1311. Sin embargo, si no se permite el tipo_solicitud_usuario en la etapa 1302, entonces se alerta al usuario del intento de acción en la etapa 1303 y de que no se permite la acción. Por lo tanto, se denegará la solicitud en la etapa 1304. Esto va seguido de llamar al agente rastreador 1102 en la etapa 1305 para registrar este evento y finaliza el proceso en la etapa 1311. A la inversa, si se permite el tipo_solicitud_usuario en la etapa 1302, entonces se permite el tipo_solicitud_usuario y se procesa en la etapa 1310.

[0054] Para el caso en donde la identidad de usuario no es la misma que la identidad de creador como se identificó en la etapa 1301, entonces se usa el campo de "confianza" en la etapa 1313. "Confianza" es la medida en la que el aprobador puede determinar si una instanciación de conjunto de registro de datos cognitivos es aceptable para el creador. Esto da el control al creador del conjunto de datos cognitivos. Si el usuario actual de los datos cognitivos no es el creador identificado en la etapa 1301, entonces en la etapa 1313 se hace una comprobación para determinar si "confianza" es igual a diez. Si "confianza" es igual a diez en la etapa 1313, entonces comienza el procesamiento para determinar si se permite el tipo de solicitud de usuario en la etapa 1302, como ya se ha explicado. Si "confianza" no es igual a diez, entonces en la etapa 1312 se llama al agente de salud 1103, y finaliza el proceso en la etapa 1311.

[0055] El fin del delator 1104 es informar al creador del conjunto de archivos de datos cognitivos. A modo de ejemplo, examínese el caso en donde el registro de datos cognitivos reside en un entorno de receptor 104. Entonces, pueden existir condiciones en las que el delator 1104 infiere una vulneración. Este evento necesita informarse al creador. De este modo, el creador puede saber quién tiene una copia de su archivo de datos cognitivos (el entorno de receptor y la identidad de usuario), obtener una copia del registro de eventos (qué ha hecho la parte de recepción con los datos) e influir en la salud del registro de datos cognitivos de la instanciación particular.

[0056] Con esto en mente, la figura 14 representa un diagrama de flujo para el proceso del agente aprobador 1107 del creador tras recibir entradas desde una instanciación del agente delator 1104, con lo que se examina el precepto 1001. Obsérvese que este agente delator no reside inicialmente en el entorno del creador, sino con la instanciación que se está procesando. El procesamiento comienza tras la recepción de un evento de llamada de delator en la etapa 1400. El aprobador 1107 lee los datos de identidad de usuario en la etapa 1401, los datos de salud en la etapa 1402 y los datos del registro de eventos de rastreador en la etapa 1403. Obsérvese que los datos del registro de eventos de rastreador se anexarán si el tamaño es demasiado grande para incrustarlos en el delator. El tamaño del delator necesita ser viable para la transmisión. En la etapa 1404, puede alertarse al creador a través de un mensaje impreso en la pantalla del creador de que existe otra instanciación del archivo de datos cognitivos, en donde en la etapa 1405 se presenta al creador la opción de indicar que esta condición está bien. De forma similar, un método alternativo para esta etapa de procesamiento, de acuerdo con la presente invención, puede ser registrar y grabar usuarios aprobados del conjunto de datos cognitivos de tal modo que el creador no tiene que procesar físicamente este acuse de recibo. Si el creador indica que la instanciación adicional es permisible en la etapa 1405, entonces el delator se devuelve con "confianza" establecida igual a diez en la etapa 1406, y finaliza el proceso en la etapa 1407. Si el creador selecciona la opción de seguir examinando el incidente de la instanciación en la etapa 1405, entonces se muestran la información de registro y los datos de registro para que el creador los examine en la etapa 1408. Una vez se han examinado, se vuelve a presentar al creador la opción en la etapa 1404 y éste indica aceptación o no en la etapa 1405. Si el creador determina que la instanciación del archivo de datos cognitivos que posee el usuario que se informa no es permisible, entonces la "confianza" se establece a cero en el delator en la etapa 1409, y se devuelve y finaliza el proceso en la etapa 1407.

[0057] Los preceptos 1001 del agente delator 1104 proceden del agente aprobador 1107 y del agente de salud 1103. El agente delator 1104 informa de vuelta a la instanciación del agente aprobador de creador 1107 tras la detección del conjunto de datos cognitivos que residen en un entorno de no creador. La dicha instanciación del agente delator 1104 que informa de vuelta al agente aprobador de creador 1107 proporciona unos medios de control para el creador para eventos tales como datos objeto de apropiación indebida o vulnerados. Esto da al creador unos medios para aprender que dichos datos han sido objeto de apropiación indebida, la identidad del autor de la apropiación indebida y unos medios para intentar la retirada de los dichos datos vulnerados. La figura 15 es un diagrama de flujo de proceso del agente delator para el precepto del agente aprobador 1107. El procesamiento comienza cuando el agente aprobador 1500 llama al agente delator. Para el caso de "confianza" igual a cero en la etapa 1501, se llama al agente de salud en la etapa 1502 para borrar la instanciación de los datos cognitivos. Para el caso en donde "confianza" es igual a diez en la etapa 1503, se llama al agente de salud en la etapa 1504 aceptando la instanciación procedente del creador. Este evento de que el delator entre en contacto con el creador puede retirarse del registro de seguimiento en la etapa 1505, entonces el proceso se termina en la etapa 1506.

[0058] Obsérvese que el agente delator necesita transmitirse entre el entorno de creador y un entorno de no creador en donde reside la instanciación del conjunto de datos cognitivos. Esto puede conseguirse abriendo el puerto de red del entorno actual y enviando el delator a la identidad de red de entorno de creador, la dirección de protocolo de Internet y la identidad de ordenador. El agente delator posee los datos de registro de agente de seguimiento que pueden ser aprovechados junto con las últimas lecturas conocidas de entorno de delator (justo antes de la transmisión de delator) para devolver el delator de vuelta al entorno de no creador.

[0059] A continuación, se examina el agente delator para el diagrama de flujo de proceso de precepto del agente de

salud 1103 de la figura 16. El procesamiento comienza tras un evento de llamada de agente de salud en la etapa 1600. Para el caso de "confianza" igual a cero en la etapa 1601, se llama al agente aprobador en la etapa 1602 para notificar al creador que se ha borrado la instanciación objeto de apropiación indebida de los datos cognitivos, y finaliza el proceso en la etapa 1609. Para el caso en donde "confianza" es igual a cinco en la etapa 1603, se llama al agente aprobador en la etapa 1604 para determinar si la instanciación de datos cognitivos es aceptable para el creador. En la etapa 1605 se hace una comprobación para determinar si se ha recibido una respuesta desde el creador. Si el creador responde, se lee el valor de "confianza" proporcionado en la respuesta de creador en la etapa 1606 y se llama al agente de salud transmitiéndole el valor de "confianza" en la etapa 1607 para su procesamiento adicional. Si el creador no ha respondido en la etapa 1605 dentro de un período de tiempo especificado, entonces se deniega la solicitud de usuario en la etapa 1608, y el proceso se termina en la etapa 1609.

[0060] Obsérvese que puede implementarse un procesamiento adicional para recibir un acuse de recibo desde el creador 1605, tal como insertar un temporizador en el proceso. Dichos temporizadores podrían usarse de una forma tal como para continuar el procesamiento después de un lapso de tiempo especificado tras la falta de recepción de acuse de recibo de creador. Adicionalmente, el entorno de creador podría implementar un registro de identidades de usuario que tienen permiso para poseer una instanciación de los datos cognitivos para automatizar este proceso.

[0061] El agente de salud determina si los datos están seguros y protegidos o en una situación comprometida. También puede determinar la vida útil de los datos y provocar que los datos cognitivos se autodestruyan. Esto se consigue supervisando el valor de "confianza" y las funciones de tiempo de procesamiento basándose en restricciones decididas por el creador. La figura 17 muestra un diagrama de flujo del agente de salud 1103. El procesamiento comienza en la etapa 1700 tras recibir una llamada de un precepto con un valor para el parámetro "confianza". Los preceptos para el agente de salud comprenden el delator, el rastreador y el aprobador. En la etapa 1701, se realiza una comprobación para determinar si el valor de "confianza" es igual a diez. Si el valor de "confianza" es igual a diez, entonces se comprueba el temporizador de datos en la etapa 1704 con la fecha/hora actual. En la etapa 1705 se hace otra comprobación para determinar si han expirado los datos cognitivos. Si han expirado, los datos se borran en la etapa 1706, y finaliza el proceso en la etapa 1708. Si no han expirado los datos en la etapa 1705, entonces se hace una llamada al proceso de acceso en la etapa 1707 pasando el "tipo_solicitud_usuario" tras lo cual finaliza el proceso en la etapa 1708. Obsérvese que esta cognición adicional se consigue para los casos de "inteligente" y "muy inteligente", en donde la "vida" de los datos puede determinarse basándose en un evento o en el tiempo.

[0062] El agente rastreador 1102 registra todos los datos de registro para el archivo de datos cognitivos manteniendo de este modo un historial de eventos de todos los eventos que tienen lugar con el archivo de datos cognitivos. Esto es extremadamente valioso tras una vulneración de seguridad, debido a que posibilita una trazabilidad. Una implementación avanzada del rastreador podría incluir informar de incidencias en tiempo real a software de seguridad u otro software de terceros, tal como software de protección antivirus o de cortafuegos, para proporcionar medidas correctivas inmediatas o estudiadas tras una vulneración.

[0063] Pueden incorporarse implementaciones de cognición avanzadas a los sistemas y métodos de la presente invención. Una capacidad valiosa es proporcionar cognición de comportamiento. Una implementación puede poseer múltiples agentes de comportamiento en donde estos agentes soportan análisis de comportamiento particulares. A modo de ejemplo, puede implementarse la cognición de comportamiento de usuario en donde la cognición puede hacer una inferencia con respecto al uso apropiado de los datos. Esta capacidad podría ayudar a detectar la conducta inapropiada y las acciones involuntarias de los empleados, que son la principal causa de vulneraciones de seguridad de datos. Esta capacidad podría por lo tanto ayudar al usuario y a la empresa a mantener la seguridad dentro de la empresa.

[0064] Considérese un empleado de empresa que usa un ordenador portátil para trabajar en las instalaciones y en diversas ubicaciones remotas. El diagrama de flujo para el agente rastreador 1102 con el precepto del AI observador 1101 en la figura 18. El procesamiento comienza en la etapa 1800 tras recibir una llamada desde el agente observador para registrar un evento tras el cual se registra una nueva entrada en los campos de asiento de registro de datos cognitivos en la etapa 1801 junto con los campos de datos de registro virtual de usuario en la etapa 1802. Se llama al agente de comportamiento en la etapa 1803 (lo que se analizará más adelante). Recuérdese que los datos de registro están compuestos por todos los campos de estructura de datos excepto el campo de "cuerpo". En este ejemplo, los campos de datos de registro virtual de usuario registran el uso de un ordenador portátil de empresa en relación con el horario de trabajo del empleado y cualquier dato *a priori*. Los campos de registro virtual son como se define a continuación:

 Registro virtual de usuario [(vs) (s) (ss) todos los campos] (nota: este campo registra el uso de ordenadores portátiles en una empresa y en ubicaciones remotas)

- Registro de uso del entorno de empresa
    - Activado
    - Terminado

- Uso de caudal

- Registro de uso del entorno remoto
  - Activado
  - Terminado
  - Uso de caudal
- Horario (entrada de empleados y confirmado basándose en análisis de uso anterior)
  - Ubicación de trabajo
  - Ubicación(es) remota(s)
  - Ubicación(es) de viaje
  - Horas (horario diario)
  - Duración
  - Historial de acceso a datos cognitivos (nota: datos de edad a partir de la estructura de datos cognitivos complementan este campo)
    - Ubicación
    - Nombre de registro de datos
    - Frecuencia
    - Con qué frecuencia

[0065] El agente de comportamiento vuelve con un valor de "confianza" que se lee en la etapa 1804. Entonces, se llama al agente de salud 1103 en la etapa 1805 pasando el parámetro "confianza" y finalizando el proceso en la etapa 1805.

[0066] El diagrama de flujo de proceso de AI de comportamiento 1108 que se representa en la figura 19 determina si el usuario (es decir, un empleado de la empresa) puede obtener acceso a datos cognitivos solicitados por el usuario desde un entorno de la empresa. Supóngase que la política de seguridad de la empresa aplica las siguientes reglas:

- Acceso a datos de nivel de seguridad "alto" y "medio" restringido al entorno de la empresa Y solo durante horas de trabajo normales, y
- Acceso restringido a datos de nivel de seguridad "bajo" restringido al entorno de la empresa Y durante horas de trabajo normales Y después de horas de trabajo normales.

[0067] El procesamiento comienza tras un evento de llamada de rastreador en la etapa 1900. En la etapa 1901 se hace una comprobación usando los datos de registro y metadatos de estructura de datos para determinar si la solicitud_usuario para acceso a datos cognitivos que se está invocando en el entorno de empresa se da durante el horario de trabajo normal del usuario. La lógica para crear reglas puede comprender:

- Horario ES lunes a viernes EN empresa
- hora_del_día_horario ES 8 a. m. HASTA 5 p. m.
- trabajo_normal ES durante horario Y hora_del_día_horario

[0068] Si la etapa 1901 determina que sí, entonces se realiza otra comprobación en la etapa 1902 para determinar si la solicitud de acceso es un comportamiento de usuario habitual. Para determinar esto, considérese el caso sencillo de leer el campo de frecuencia del registro virtual de usuario, en donde se actualiza un indicador para cada iteración de acceso de usuario a la instanciación de datos. Un ejemplo de lógica para construir reglas para el "comportamiento de usuario habitual" sería el siguiente:

- SI frecuencia ES MAYOR QUE 2 Y con_qué_frecuencia ES MAYOR QUE dos_veces_al_día ENTONCES comportamiento_usuario IGUAL A habitual
- SI NO comportamiento_usuario IGUAL A no_habitual

[0069] Unos eventos de registro *a priori* pueden usarse para determinar si el usuario ha accedido antes a estos datos. Si se determina que el comportamiento de usuario es "habitual", entonces la "confianza" se iguala a diez en la etapa 1903, y finaliza el proceso en la etapa 1904. Si el comportamiento de usuario es "no habitual" en la etapa 1902, entonces la "confianza" se iguala a cero en la etapa 1906, y finaliza el proceso en la etapa 1904. Para el resto de la política de seguridad, si la hora actual no cae dentro del horario normal de trabajo en la etapa 1901, entonces se realiza otra comprobación en la etapa 1905 para determinar el nivel de seguridad. Si el nivel de seguridad es bajo en la etapa 1905, entonces "confianza" se equipara a diez en la etapa 1903, y finaliza el proceso 1904. Sin embargo, si la seguridad es "alta" o "media" en la etapa 1905, entonces la "confianza" se iguala a cero en la etapa 1906, y finaliza

el proceso en la etapa 1904. Puede aplicarse una lógica similar para el caso del empleado que trabaja a distancia (es decir, el ordenador portátil que solicita el acceso no está en la ubicación de empresa). Si se determina que el usuario realiza una vulneración o un comportamiento erróneo, se notifica al creador. Esta capacidad puede ser valiosa para entornos corporativos o de agencias gubernamentales que deben asegurar la seguridad de datos.

[0070] Otro enfoque para la implementación de software es crear una capacidad *adaptativa*, datos cognitivos adaptativos, empleando técnicas y algoritmos de inteligencia artificial (IA). Estas implementaciones sustituyen o aumentan el procesamiento de von Neumann divulgado anteriormente. Pueden implementarse funcionalidades y potenciaciones adicionales basándose en lo inteligente que el creador desee que se vuelvan los datos cognitivos, en lo adaptativos que sea necesario que sean los datos cognitivos y en qué conocimientos adicionales deberían tener los datos cognitivos para satisfacer las necesidades del creador.

[0071] La IA puede implementarse en todo el MAS. A modo de ejemplo, considérese la determinación de "confianza" en donde los datos cognitivos razonan "¿confío en el usuario?". Este razonamiento adaptativo puede implementarse usando una disciplina de la IA denominada lógica de inferencia difusa (FI), que posee los antecedentes del horario de trabajo del usuario, la ubicación actual del usuario en el entorno y el uso histórico del usuario de la instanciación de datos cognitivos, y similares. Para usar el sistema de FI pueden emplearse los siguientes parámetros:

- Hora del día
- Horas del horario de trabajo diario del usuario
- Dirección de IP/datos de identificación de red actual del entorno
- Direcciones de IP/datos de identificación de red pasados del entorno
- Frecuencia de acceso de usuario a datos cognitivos

[0072] El sistema de FI puede procesar estas entradas para determinar el nivel de confianza, en donde la confianza es la salida del sistema de FI. Los valores de salida de FI nítidos para la confianza son X(0, 5, 10) cumpliendo con la lógica divulgada en el presente documento.

[0073] Las funciones de pertenencia de FI se proporcionan en las figuras 20, 21 y 22. El grado de pertenencia de estas funciones varía en Y(0, 1). En la figura 20, la pertenencia del horario de trabajo clasifica las funciones de pertenencia basándose en las horas de trabajo del usuario (es decir, la hora del día). La función 2001, desde 12 a. m. hasta aproximadamente 6 a. m. se clasifica como "tiempo de trabajo no normal a primera hora del día"; la función 2002 muestra un intervalo de aproximadamente 7 a. m. hasta aproximadamente 6 p. m., y se clasifica como "tiempo de trabajo normal"; y el tiempo de trabajo después de aproximadamente 6 p. m. mostrado como la función 2003 se considera "un tiempo de trabajo no normal a última hora del día".

[0074] La figura 21 implementa la inferencia de los datos cognitivos acerca de la ubicación de entorno basándose en datos *a priori* acerca de la ubicación y la frecuencia de acceso del usuario desde esa ubicación. La primera función 2101 representa no reconocer el entorno de usuario remoto (es decir, comprobando la dirección de IP y la información de red y no hallando la misma en el registro de eventos). La función de pertenencia 2101 representa que la ubicación remota nunca se ha usado antes y hasta que la ubicación se ha usado un par de veces. Una vez se han usado en ocasiones adicionales, alrededor de dos a cinco veces, los datos "conocen algo" el entorno remoto, y la función 2102 (según la representación de la función de pertenencia) se usa para representar esta instancia. Si el usuario continúa utilizando repetidamente la ubicación remota, después de cinco veces el entorno se vuelve "conocido" para los datos, y la función se representa como la función 2103. Por supuesto, pueden usarse otras etiquetas y funciones para denotar el grado con el que el sistema reconoce el entorno del usuario remoto, y pueden usarse diferentes valores y marcos temporales con los que llegar a las determinaciones de "remoto no conocido", "remoto algo conocido" y "remoto conocido". Adicionalmente, si la localización es en la empresa en donde trabaja el usuario, el archivo de datos "conoce" el entorno, lo cual es una función de pertenencia inferida, debido a que la frecuencia de uso debería ser un número elevado.

[0075] Del mismo modo, la figura 22 implementa las funciones de pertenencia de los datos cognitivos alrededor de lo bien que los datos conocen al usuario. Esto se basa en la frecuencia con la que el usuario accede a los datos. Los datos no consideran al usuario "conocido" si el usuario ha accedido a los mismos menos de aproximadamente cuatro veces, como es mostrado por la función 2201; los datos consideran al usuario "algo conocido" si el usuario accede a los datos aproximadamente de cuatro a siete veces, lo que es mostrado por la función 2202; y los datos consideran al usuario "conocido" si el usuario accede a los mismos más de aproximadamente siete veces, lo que es mostrado por la función 2203. Como se ha esbozado anteriormente con respecto a la localización remota, pueden usarse otras etiquetas y funciones para denotar el grado con el que el sistema reconoce al usuario, y pueden usarse diferentes valores y frecuencia de acceso con los que llegar a las determinaciones de "usuario no conocido", "usuario algo conocido" y "usuario conocido". En el ejemplo anterior, estos antecedentes de FI se usan para aplicar las siguientes reglas:

SI tiempo_normal Y entorno_no_conocido_remoto Y usuario_conocido ENTONCES confianza = 5;
SI tiempo_normal Y entorno_algo_conocido_remoto Y usuario_conocido ENTONCES confianza = 5;
SI tiempo_normal Y entorno_conocido_remoto Y usuario_conocido ENTONCES confianza = 10;

SI tiempo_normal Y entorno_empresa Y usuario_conocido ENTONCES confianza = 10;
SI no_normal_primera_hora O no_normal_última_hora Y entorno_no_conocido_remoto Y usuario_conocido ENTONCES confianza = 0;
SI no_normal_primera_hora O no_normal_última_hora Y entorno_algo_conocido_remoto Y usuario_conocido ENTONCES confianza = 5;
SI no_normal_primera_hora O no_normal_última_hora Y entorno_conocido_remoto Y usuario_conocido ENTONCES confianza = 10;
SI no_normal_primera_hora O no_normal_última_hora Y entorno_empresa Y usuario_conocido ENTONCES confianza = 10;
SI tiempo_normal Y entorno_no_conocido_remoto Y usuario_no_conocido ENTONCES confianza = 0;
SI tiempo_normal Y entorno_algo_conocido_remoto Y usuario_no_conocido ENTONCES confianza = 0;
SI tiempo_normal Y entorno_conocido_remoto Y usuario_no_conocido ENTONCES confianza = 5;
SI tiempo_normal Y entorno_empresa Y usuario_no_conocido ENTONCES confianza = 5;
SI no_normal_primera_hora O no_normal_última_hora Y entorno_no_conocido_remoto Y usuario_no_conocido ENTONCES confianza = 0;
SI no_normal_primera_hora O no_normal_última_hora Y entorno_algo_conocido_remoto Y usuario_no_conocido ENTONCES confianza = 0;
SI no_normal_primera_hora O no_normal_última_hora Y entorno_conocido_remoto Y usuario_no_conocido ENTONCES confianza = 0;
SI no_normal_primera_hora O no_normal_última_hora Y entorno_empresa Y usuario_no_conocido ENTONCES confianza = 0;
SI tiempo_normal Y entorno_no_conocido_remoto Y usuario_algo_conocido ENTONCES confianza = 0;
SI tiempo_normal Y entorno_algo_conocido_remoto Y usuario_algo_conocido ENTONCES confianza = 0;
SI tiempo_normal Y entorno_conocido_remoto Y usuario_algo_conocido ENTONCES confianza = 5;
SI tiempo_normal Y entorno_empresa Y usuario_algo_conocido ENTONCES confianza = 10;
SI no_normal_primera_hora O no_normal_última_hora Y entorno_no_conocido_remoto Y usuario_algo_conocido ENTONCES confianza = 0;
SI no_normal_primera_hora O no_normal_última_hora Y entorno_algo_conocido_remoto Y usuario_algo_conocido ENTONCES confianza = 0;
SI no_normal_primera_hora O no_normal_última_hora Y entorno_conocido_remoto Y usuario_algo_conocido ENTONCES confianza = 5;
SI no_normal_primera_hora O no_normal_última_hora Y entorno_empresa Y usuario_algo_conocido ENTONCES confianza = 10;

[0076] La figura 23 representa el diagrama de flujo del procesamiento singular requerido para soportar el procesamiento de FI. Se hacer notar que el mismo flujo de procesamiento inicial representado en la figura 11 puede emplearse para supervisar un evento de cambio de estado. Posteriormente, tras una determinación de "confianza", puede invocarse el procesamiento de FI de la figura 23, en donde el procesamiento comienza tras una solicitud para determinar la "confianza" en la etapa 2300. En la etapa 2301, la hora_del_día se lee del reloj del sistema del entorno; frecuencia_usuario del usuario que accede a los datos se lee del registro virtual; se lee información de identificación de entorno_actual; e instancias pasadas del entorno_actual registradas en el registro de eventos se suman para obtener las entradas nítidas en el sistema de FI.

[0077] En la etapa 2302, se hace una comprobación para determinar si la identificación de entorno actual se ubica en la red de instalaciones de la empresa. Si se corrobora que la identidad está en la empresa, entonces el valor de ubicación_usuario se establece a 10 en la etapa 2303. Si no es así, se realiza otra comprobación en la etapa 2304 para determinar si el entorno actual está en el registro de eventos. Si el registro de eventos produjo cero eventos del entorno actual del usuario, entonces, la ubicación del usuario se establece a cero en la etapa 2305 indicando que el entorno no es conocido por los datos. De lo contrario, la suma total de veces que el usuario accedió a los datos en su entorno actual se establece en la etapa 2306, y el proceso continúa en la etapa 2307.

[0078] La hora_del_día, la ubicación_usuario y la frecuencia_usuario son las entradas nítidas al proceso de difuminación en donde se generan las funciones de pertenencia de FI en la etapa 2307. Entonces se aplican las reglas de FI en la etapa 2308. La regla que brinda el resultado más fuerte se considera el operador funcional consecuente que determina el valor para la "confianza". Una vez que se ha aplicado la regla más fuerte, se obtiene el valor nítido para la "confianza" en la etapa 2309, y finaliza el proceso en la etapa 2310.

[0079] Para fines de análisis, y no para fines de limitación, la figura 24 muestra una implementación de hardware de alto nivel del sistema de datos cognitivos de la figura 2. Un sistema computacional digital 2400 emplea una unidad de procesamiento 2402. Sin embargo, las funciones indicadas en la figura 2 pueden integrarse conjuntamente o encapsularse por separado en numerosas configuraciones como se describe más adelante. Estas configuraciones pueden variar desde unidades de microcontroladores hasta sistemas de ordenadores personales, estaciones de trabajo empresariales, servidores, pasarelas, sistemas de red y/o cualquier otro hardware que acepte y procese datos.

[0080] Con referencia a la figura 24, un sistema ilustrativo para implementar la forma de realización divulgada incluye un dispositivo de computación o módulos de computación, tales como un dispositivo de computación digital 2400. La

configuración básica del dispositivo informático 2400 comprende al menos una unidad de procesamiento 2402, una memoria extraíble 2405, una memoria fija local 2406 que comprende memoria de acceso aleatorio (RAM) y memoria de solo lectura (ROM) y memoria de sistema de disco duro. Las configuraciones de memoria del sistema varían, pero habitualmente incluyen los elementos de memoria expuestos. El dispositivo informático incluye también un sistema operativo 2403 y una pluralidad de aplicaciones y procesos 2404. El dispositivo informático 2400 también puede comprender un(os) dispositivo(s) de entrada/salida (E/S) 2408 tales como teclado, ratón, lápiz y dispositivo de entrada de voz, dispositivo de entrada táctil, una pantalla, altavoces, impresora, etc. Otros dispositivos digitales 2409 interactúan con el dispositivo informático 2400 a través de los puertos de comunicación de dispositivo informático 2407. Estos dispositivos adicionales de almacenamiento de datos (extraíbles y/o no extraíbles) pueden comprender, por ejemplo, discos magnéticos o discos ópticos, impresoras, módems, etc. Los medios de almacenamiento informático comprenden, pero sin limitación, RAM, ROM, EEPROM, memoria flash u otra tecnología de memoria, CD-ROM, discos versátiles digitales (DVD) u otro almacenamiento óptico, casetes magnéticos, cinta magnética, almacenamiento en disco magnético u otros dispositivos de almacenamiento magnético, o cualquier otro medio que pueda usarse para almacenar la información deseada y al que pueda accederse mediante el dispositivo informático 2400. Cualquier medio de almacenamiento informático de este tipo puede ser parte del dispositivo 2400.

[0081] Para describir claramente las funciones de soporte de hardware requeridas para el sistema de datos cognitivos 2400 de la figura 24, se explica el siguiente ejemplo de las etapas realizadas tras utilizar el marco de datos cognitivos junto con detalles que se refieren al hardware. El sistema y método de datos cognitivos 2400 comprende módulos de software o hardware codificados de acuerdo con los diagramas de flujo de las figuras 3-18. Este código se almacena en la memoria dentro del controlador 2400 en una forma de realización y puede almacenarse en un medio legible por ordenador con instrucciones codificadas en el mismo para ser leído por el sistema de datos cognitivos 2400. Cuando son ejecutadas por la unidad de procesamiento 2402, estas instrucciones hacen que la unidad de procesamiento implemente las etapas expuestas en los diagramas de flujo de las figuras 3-18. Se accede a los datos y estos se almacenan utilizando la memoria extraíble 2405 y/o la memoria fija local 2406 para ejecutar el software de aplicación de marco de datos cognitivos 2401, así como otras aplicaciones y procesos 2404 (por ejemplo, otras aplicaciones de software tales como Explorador de Windows, software Microsoft Office y similares). El marco de datos cognitivos puede implementarse como una aplicación de software "autónoma" o puede ser una aplicación "de extensión". Si el marco de datos cognitivos es una aplicación "de extensión", se accedería a la capacidad a través de otras aplicaciones de software de terceros 2404. Por ejemplo, si la aplicación del marco de datos cognitivos es una "extensión" para el producto de procesamiento de Microsoft Word, esta podría proporcionar la funcionalidad divulgada en el presente documento ofreciendo una opción de datos cognitivos al usuario.

[0082] El sistema operativo 2403 traduce las instrucciones a acciones ejecutables que hacen que el hardware del sistema 2401 y otros dispositivos 2409 respondan y funcionen de acuerdo con dicho código ejecutable. Otros dispositivos digitales 2409 se conectan al sistema 2400 a través de los puertos de comunicación 2408 mediante hardware o de forma inalámbrica. El software de marco de datos cognitivos 2401 supervisa los puertos de entrada/salida de hardware 2407, tales como un teclado y/o ratón, para la selección de creador o usuario. Tras recibir una solicitud de creador o de usuario desde un dispositivo de entrada/salida 2407, se invocan las instrucciones de software de marco de datos cognitivos 2401. La RAM/ROM 2406 proporciona la memoria necesaria para soportar la carga de las instrucciones ejecutables y memoria para soportar el procesamiento en tiempo real. La unidad de procesamiento 2402 que ejecuta el código de marco de datos cognitivos 2401 accede a la memoria de almacenamiento de datos 2405 para soportar ejecuciones de software y la ejecución de las instrucciones. En una forma de realización, los recursos y repositorio de datos cognitivos se usan para almacenar datos y recursos cognitivos como una sección de la memoria 2406. Tras detectar la selección de creador o usuario, el estado de los datos cognitivos almacenados en la memoria 2406 u otras capacidades de memoria del dispositivo digital 2409 cambia de latente a "activo" o "en movimiento". La configuración de entorno computacional se compara y se configura de acuerdo con la configuración indicada en los campos de registro y metadatos de los datos cognitivos almacenados para soportar el nivel de inteligencia y el nivel de seguridad indicados por dichos datos cognitivos almacenados. Para alcanzar estos niveles de seguridad e inteligencia, los recursos pueden cerrarse o activarse en consecuencia (por ejemplo, el puerto de Internet 2408/2409 puede cerrarse para alcanzar el nivel de seguridad indicado requerido para activar y acceder a los recursos de archivos de datos cognitivos almacenados). Los puertos se gestionan (es decir, se abren y se cierran) posteriormente para transmitir software de un entorno a otro como es el caso para la transmisión del software de delator desde un entorno de recepción al entorno de creador y viceversa, proporcionando de este modo un control remoto para el creador de una instanciación de sus datos en un entorno de no creador.

[0083] El método y sistema divulgados protege ventajosamente la exposición del usuario a actividad no deseada y maliciosa empleando mecanismos de control avanzados implementados en o cerca del dispositivo computacional en una forma de realización. La metodología y sistema de datos cognitivos permite que el consumidor tome proactivamente el control de quién, cómo, cuándo y si otra parte puede poseer sus datos. Ventajosamente, la metodología divulgada transforma datos desde un archivo pasivo que puede ser obtenido, comprometido y usado indebidamente por cualquiera a un archivo de datos adaptativo, consciente y autocontrolable que posibilita la autogestión ofreciendo al creador protección y seguridad. Esta capacidad puede personalizar datos cognitivos según las prioridades del creador. También proporciona medios inteligentes para una configuración singular del entorno para proteger los datos mientras está en uso. Los datos cognitivos se gestionan y se controlan dependiendo del entorno, el estado, la seguridad, la salud y el nivel de inteligencia de la instanciación de datos cognitivos particular. De este modo,

se capacita al usuario para tomar el control sobre y limitar el acceso a sus datos.

[0084] Aunque se han mostrado a modo de ilustración solo ciertas características preferidas de la invención, a los expertos en la materia se les ocurrirán muchas modificaciones y cambios. Por ejemplo, otra forma de realización solo puede procesar datos seleccionados o quitados como datos cognitivos, mientras que todos los otros datos pueden no considerarse necesarios para que se vuelvan inteligentes. Esta invención pretende proporcionar el fundamento que habilite la cognición de datos. Pueden llevarse a cabo otros procesos avanzados aprovechando la capacidad de cognición divulgada, lo que puede comprender AI adicionales para aumentar las características de cognición. Ha de entenderse, por lo tanto, que se pretende que las presentes reivindicaciones cubran todas las modificaciones y cambios de este tipo que caigan dentro del alcance de la invención.

[0085] Los dispositivos y subsistemas de las formas de realización ilustrativas de las figuras 1-24 son para fines ilustrativos, debido a que son posibles muchas variaciones del hardware específico usado para implementar las formas de realización ilustrativas, como será apreciado por los expertos en las materias pertinentes. Por ejemplo, la funcionalidad de uno o varios de los dispositivos y subsistemas de las formas de realización ilustrativas de las figuras 1-24 puede implementarse a través de uno o más sistemas o dispositivos informáticos programados.

[0086] Para implementar tales variaciones, así como otras variaciones, un único sistema informático puede programarse para realizar las funciones de propósito especial de uno o varios de los dispositivos y subsistemas de las formas de realización ilustrativas de las figuras 1-24. Por otra parte, dos o más sistemas o dispositivos informáticos programados pueden sustituir a cualquiera de los dispositivos y subsistemas de las formas de realización ilustrativas de las figuras 1-24. En consecuencia, los principios y ventajas de un procesamiento distribuido, tales como redundancia, replicación y similares, también pueden implementarse, según se desee, para aumentar la robustez y el rendimiento de los dispositivos y subsistemas de las formas de realización ilustrativas de las figuras 1-24.

[0087] Los dispositivos y subsistemas de las formas de realización ilustrativas de las figuras 1-24 pueden almacenar información en relación con diversos procesos descritos en el presente documento. Esta información puede almacenarse en una o más memorias, tales como un disco duro, un disco óptico, un disco magneto-óptico, una memoria RAM, y similares, de los dispositivos y subsistemas de las formas de realización ilustrativas de las figuras 1-24. Una o más bases de datos de los dispositivos y subsistemas de las formas de realización ilustrativas de las figuras 1-24 pueden almacenar la información usada para implementar las formas de realización ilustrativas de la presente invención. Las bases de datos pueden organizarse usando estructuras de datos (por ejemplo, registros, tablas, matrices, campos, gráficos, árboles, listas y similares) incluidas en una o más memorias o dispositivos de almacenamiento enumerados en el presente documento. Los procesos descritos con respecto a las formas de realización ilustrativas de las figuras 1-24 pueden incluir estructuras de datos apropiadas para almacenar los datos recogidos y/o generados por los procesos de los dispositivos y subsistemas de las formas de realización ilustrativas de las figuras 1-24 en uno o más bancos de datos de la misma.

[0088] Todos los dispositivos y subsistemas de las formas de realización ilustrativas de las figuras 1-24, o una porción de los mismos, pueden implementarse convenientemente usando uno o más sistemas informáticos de propósito general, microprocesadores, procesadores de señales digitales, microcontroladores y similares, programados de acuerdo con las enseñanzas de las formas de realización ilustrativas de la presente invención, como será apreciado por los expertos en las técnicas de la informática y el software. Un software apropiado puede ser preparado fácilmente por programadores expertos basándose en las enseñanzas de las formas de realización ilustrativas, como será apreciado por los expertos en la técnica del software. Además, los dispositivos y subsistemas de las formas de realización ilustrativas de las figuras 1-24 pueden implementarse en la red mundial. Además, los dispositivos y subsistemas de las formas de realización ilustrativas de las figuras 1-24 pueden implementarse mediante la preparación de circuitos integrados específicos de la aplicación o interconectando una red apropiada de circuitos de componentes convencionales, como será apreciado por los expertos en las técnicas de la electricidad. Por lo tanto, las formas de realización ilustrativas no se limitan a ninguna combinación específica de circuitería de hardware y/ software.

[0089] Como se ha expuesto anteriormente, los dispositivos y subsistemas de las formas de realización ilustrativas de las figuras 1-24 pueden incluir medios legibles por ordenador o memorias para contener instrucciones programadas de acuerdo con las enseñanzas de la presente invención y para contener estructuras de datos, tablas, registros, y/u otros datos descritos en el presente documento. Los medios legibles por ordenador pueden incluir cualquier medio adecuado que participe en la provisión de instrucciones a un procesador para su ejecución. Un medio de este tipo puede adoptar muchas formas, incluyendo, aunque sin limitación, medios no volátiles, medios volátiles, medios de transmisión y similares. Los medios no volátiles pueden incluir, por ejemplo, discos ópticos o magnéticos, discos magneto-ópticos y similares. Los medios volátiles pueden incluir memorias dinámicas y similares. Los medios de transmisión pueden incluir cables coaxiales, hilo de cobre, fibra óptica y similares. Los medios de transmisión también pueden adoptar la forma de ondas acústicas, ópticas, electromagnéticas y similares, tales como las generadas durante comunicaciones por radiofrecuencia (RF), comunicaciones de datos por infrarrojos (IR) y similares. Las formas comunes de medios legibles por ordenador pueden incluir, por ejemplo, un disquete, un disco flexible, disco duro, cinta magnética, cualquier otro medio magnético adecuado, un CD-ROM, CDRW, DVD, cualquier otro medio óptico adecuado, tarjetas perforadas, cinta de papel, láminas de marcas ópticas, cualquier otro medio físico adecuado con

patrones de agujeros u otro signo ópticamente reconocible, una RAM, una PROM, una EPROM, una FLASH-EPROM, cualquier otro chip o cartucho de memoria adecuado, una onda portadora, o cualquier otro medio adecuado del que puede leer un ordenador.

[0090] Aunque las presentes invenciones se han descrito en relación con un número de formas de realización e implementaciones ilustrativas, las presentes invenciones no se limitan a ello, sino que abarcan diversas modificaciones, y disposiciones equivalentes, que caen dentro del ámbito de futuras reivindicaciones.

REIVINDICACIONES

1. Un método para seguridad de datos autónoma y adaptativa mediante procesamiento de datos, que comprende:
ejecutar en un procesador un archivo de datos cognitivos, siendo el archivo de datos cognitivos un archivo informático que comprende medios de seguridad autónomos incrustados en datos para asegurar los datos, en donde el procesador está configurado para realizar etapas que comprenden:

establecer un estado latente inicial para los datos de entre una pluralidad de estados que incluyen latente, activo y en movimiento;
supervisar en busca de un evento de cambio de estado de los datos a un estado activo o en movimiento;
registrar el evento de cambio de estado y campos de estructura de datos en memoria junto con metadatos que describen el estado de datos, en donde los metadatos contienen al menos información del creador de datos, información de usuario actual e información de entorno de datos actual;
establecer una indicación de grado de confianza de una instanciación de datos basándose en dicho evento de cambio de estado y dichos campos de estructura de datos, en donde el grado de confianza incluye al menos uno de un grado de certidumbre o nivel de certeza de que se permite la instanciación de datos;
determinar y aplicar requisitos de seguridad para permitir que un usuario acceda a contenidos de la instanciación de datos basándose en el grado de confianza de la instanciación de datos; y
gestionar y controlar el entorno computacional de dichos datos basándose en los requisitos de seguridad.

2. El método de la reivindicación 1, en donde establecer el grado de confianza comprende además:

enviar al creador una alerta del evento tras el establecimiento de un grado de confianza bajo, en donde la alerta del evento incluye la información de usuario actual; y
retirar de la memoria la instanciación de datos.

3. El método de la reivindicación 1, en donde establecer el grado de confianza comprende además:

enviar al creador una alerta del evento tras el establecimiento de un grado de confianza medio, en donde la alerta del evento incluye la información de usuario actual; y
solicitar al creador que apruebe o rechace la posesión de la instanciación de datos por el usuario actual, en donde, si el creador aprueba que el usuario posea la instanciación de datos, el grado de confianza se restablece a alto, y si el creador rechaza que el usuario posea la instanciación de datos, el grado de confianza se restablece a bajo.

4. El método de la reivindicación 1, en donde establecer el grado de confianza comprende además:
conceder al usuario acceso a la instanciación de datos tras el establecimiento de un grado de confianza alto.

5. El método de la reivindicación 1, en donde establecer el grado de confianza se basa en al menos uno de los comportamientos de usuario, comportamiento de datos y comportamiento de entorno.

6. Un sistema para procesar datos en un entorno computacional para proporcionar seguridad de datos autónoma y adaptativa, que comprende lo siguiente:

uno o más procesadores; y
una memoria acoplada operativamente a los uno o más procesadores que están configurados para ejecutar instrucciones programadas almacenadas en la memoria que comprenden:

supervisar un estado de un archivo de datos cognitivos, siendo el archivo de datos cognitivos un archivo informático que comprende medios de seguridad autónomos incrustados en datos para asegurar los datos, incluyendo el archivo de datos cognitivos al menos una de información del creador, información de usuario e información del entorno computacional del usuario;
procesar el archivo de datos cognitivos basándose en requisitos de seguridad de datos y en el entorno de cómputo de usuario para establecer información de seguridad de datos;
determinar una indicación o grado de confianza de una instanciación de datos en donde el grado de confianza incluye al menos uno del grado de certidumbre o nivel de certeza de que se permite la instanciación de datos;
establecer o controlar puertos en el entorno computacional del usuario y procesos que se usan junto con el procesamiento de archivo de datos cognitivos; y
cerrar, bloquear o controlar los puertos abiertos en el entorno computacional del usuario y procesos que no se usan junto con el procesamiento de archivo de datos cognitivos; y
almacenar un evento de usuario asociado al archivo de datos cognitivos.

7. El sistema de la reivindicación 6, que comprende además usar el grado de confianza de la instanciación de datos para determinar una función del sistema.

8. El sistema de la reivindicación 7, que comprende además determinar una pluralidad de grados de confianza de la instanciación de datos.

9. El sistema de la reivindicación 7, en donde dicha función de sistema se selecciona de entre el grupo que consiste en si permitir una instanciación de datos; si autodestruir un archivo; si autoarchivar un archivo; si limitar el número de veces que puede accederse a un archivo; si limitar el tiempo durante el cual un archivo puede permanecer abierto; si quitar del archivo algunos de los datos; si y cómo aplicar un agente inteligente observador; si y cómo aplicar un agente inteligente rastreador; si y cómo aplicar un agente inteligente de comportamiento; si y cómo aplicar un agente inteligente de salud; si y cómo aplicar un agente inteligente delator; y si y cómo aplicar un agente inteligente aprobador.

10. El sistema de la reivindicación 6, en donde la etapa de determinar una pluralidad de grados de confianza determina un grado de confianza que es al menos uno de unos niveles de confianza bajo, medio y alto.

11. El sistema de la reivindicación 6, en donde la etapa de determinar el grado de confianza de la instanciación de datos determina un grado de confianza basándose en al menos uno de los comportamientos de usuario, comportamiento de datos y comportamiento de entorno.

12. El sistema de la reivindicación 6, en donde el tipo de archivo de datos se selecciona de entre al menos uno de un tipo de medios digitales, un tipo multimedia, un tipo de base de datos, un tipo de archivo digital y un tipo de documento.

13. Un medio legible por ordenador que tiene almacenadas en el mismo instrucciones para procesar un archivo de datos cognitivos para proporcionar seguridad de datos autónoma y adaptativa, siendo dicho archivo de datos cognitivos un archivo informático que comprende un código de seguridad ejecutable por máquina autónoma incrustado en datos para asegurar los datos, que, cuando es ejecutado por un procesador, hace que el procesador realice etapas que comprenden:

establecer un estado latente inicial para los datos de entre una pluralidad de estados que incluyen latente, activo y en movimiento;
supervisar en busca de un evento de cambio de estado de los datos a un estado activo o en movimiento;
registrar el evento de cambio de estado y campos de estructura de datos en memoria;
establecer una indicación o grado de confianza de una instanciación de datos basándose en dicho evento de cambio de estado y dichos campos de estructura de datos, en donde el grado de confianza incluye al menos uno de un grado de certidumbre o nivel de certeza de que se permite la instanciación de datos;
determinar y aplicar requisitos de seguridad para permitir que un usuario acceda a contenidos de la instanciación de datos basándose en el grado de confianza de la instanciación de datos; y
gestionar y controlar el entorno computacional de dichos datos basándose en los requisitos de seguridad.

14. El medio legible por ordenador de la reivindicación 13, en donde establecer el grado de confianza comprende además:

enviar al creador una alerta del evento tras el establecimiento de un grado de confianza bajo, en donde la alerta del evento incluye la información del usuario actual; y
retirar de la memoria la instanciación de datos.

15. El medio legible por ordenador de la reivindicación 13, en donde establecer el grado de confianza comprende además:

enviar al creador una alerta del evento tras el establecimiento de un grado de confianza medio, en donde la alerta del evento incluye la información de usuario actual; y
solicitar al creador que apruebe o rechace la posesión de la instanciación de datos por el usuario actual, en donde, si el creador aprueba que el usuario posea la instanciación de datos, el grado de confianza se restablece a alto, y si el creador rechaza que el usuario posea la instanciación de datos, el grado de confianza se restablece a bajo.

16. El medio legible por ordenador de la reivindicación 13, en donde establecer el grado de confianza comprende además:
conceder al usuario acceso a la instanciación de datos tras el establecimiento de un grado de confianza alto.

17. El medio legible por ordenador de la reivindicación 13, en donde establecer el grado de confianza se basa en al menos uno de los comportamientos de usuario, comportamiento de datos y comportamiento de entorno.

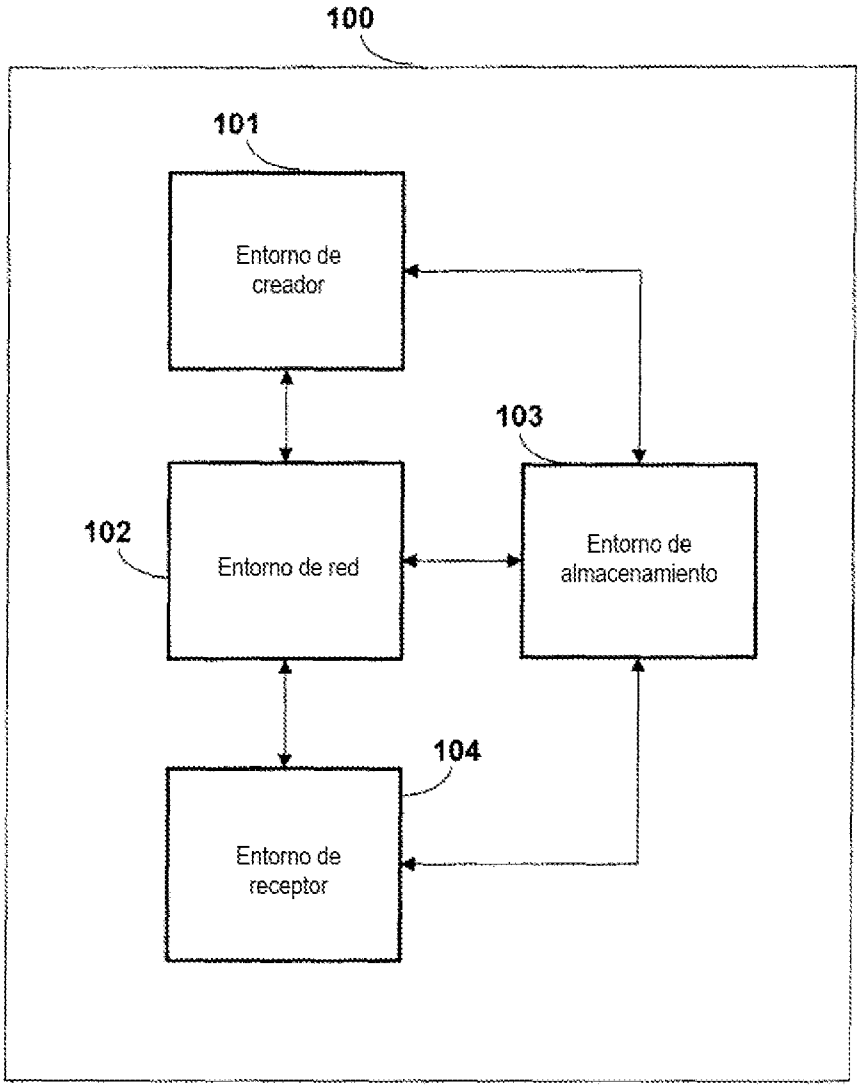
Entornos de datos cognitivos
100
101
Entorno de creador
103
102
Entorno de red
Entorno de almacenamiento
104
Entorno de receptor

Fig. 1

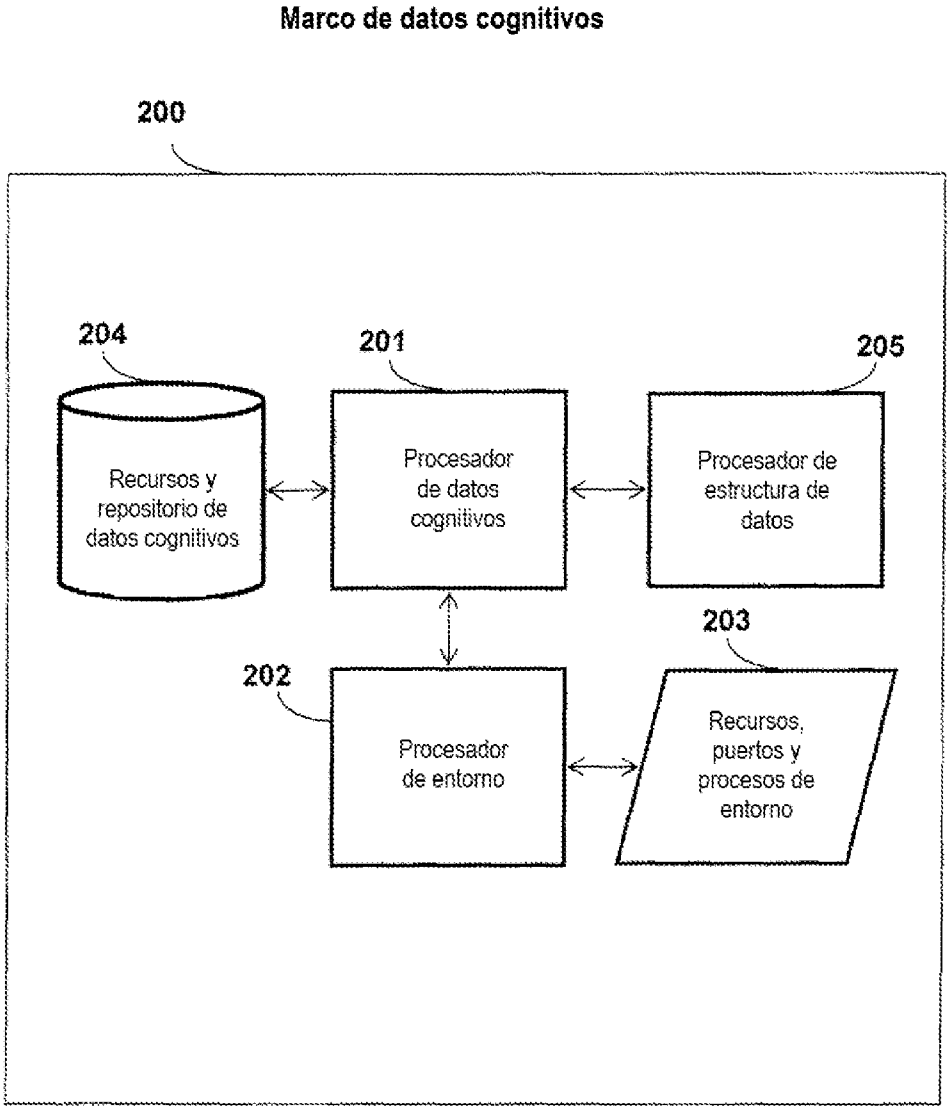
Marco de datos cognitivos
200
204
201
205
Recursos y repositorio de datos cognitivos
Procesador de datos cognitivos
Procesador de estructura de datos
203
202
Procesador de entorno
Recursos, puertos y procesos de entorno

Fig. 2

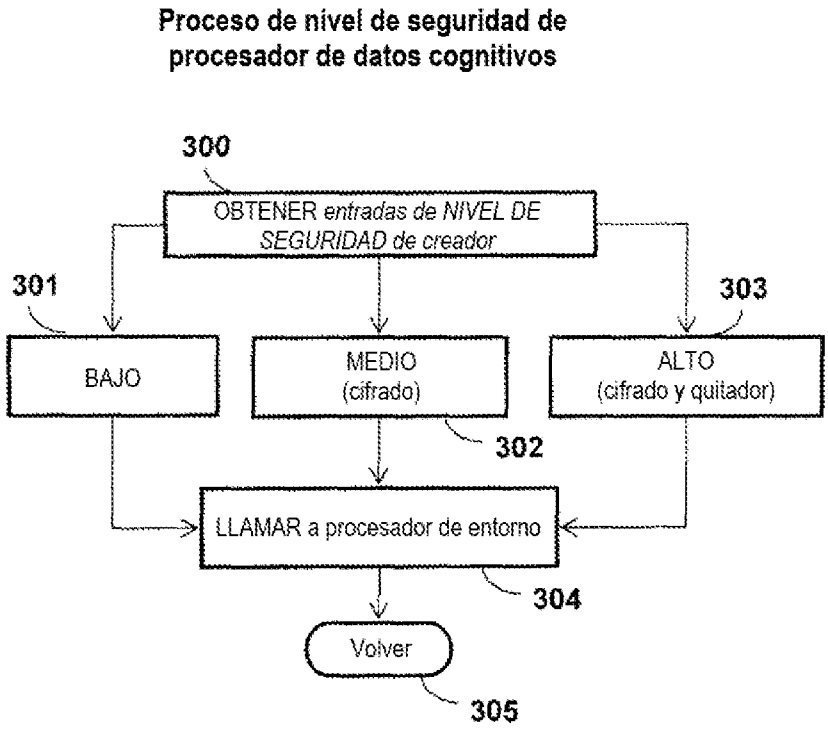
Proceso de nivel de seguridad de procesador de datos cognitivos
300
OBTENER entradas de NIVEL DE SEGURIDAD de creador
301
303
BAJO
MEDIO (cifrado)
ALTO (cifrado y quitador)
302
LLAMAR a procesador de entorno
304
Volver
305

Fig. 3

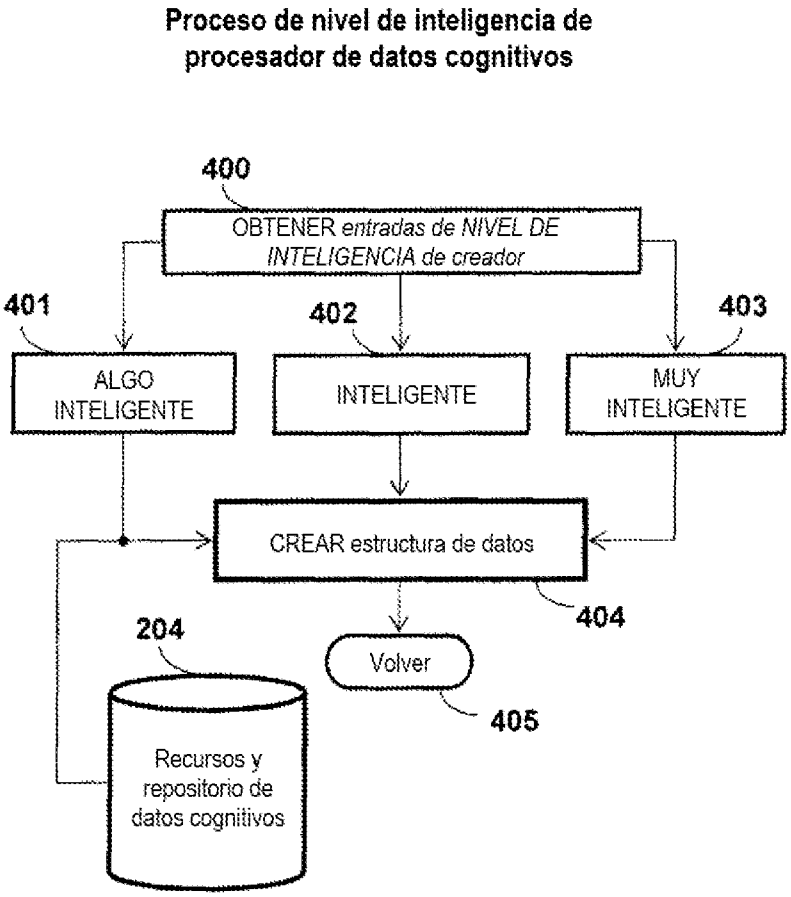
Proceso de nivel de inteligencia de procesador de datos cognitivos
400
OBTENER entradas de NIVEL DE INTELIGENCIA de creador
401
402
403
ALGO INTELIGENTE
INTELIGENTE
MUY INTELIGENTE
CREAR estructura de datos
404
204
Volver
405
Recursos y repositorio de datos cognitivos

Fig. 4

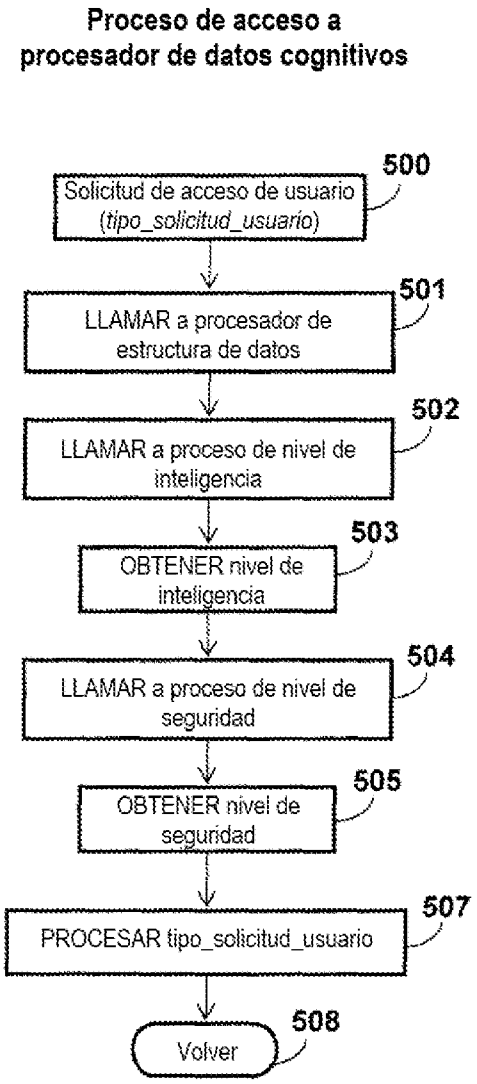
Proceso de acceso a procesador de datos cognitivos
500
Solicitud de acceso de usuario (tipo_solicitud_usuario)
501
LLAMAR a procesador de estructura de datos
502
LLAMAR a proceso de nivel de inteligencia
503
OBTENER nivel de inteligencia
504
LLAMAR a proceso de nivel de seguridad
505
OBTENER nivel de seguridad
507
PROCESAR tipo_solicitud_usuario
508
Volver

Fig. 5

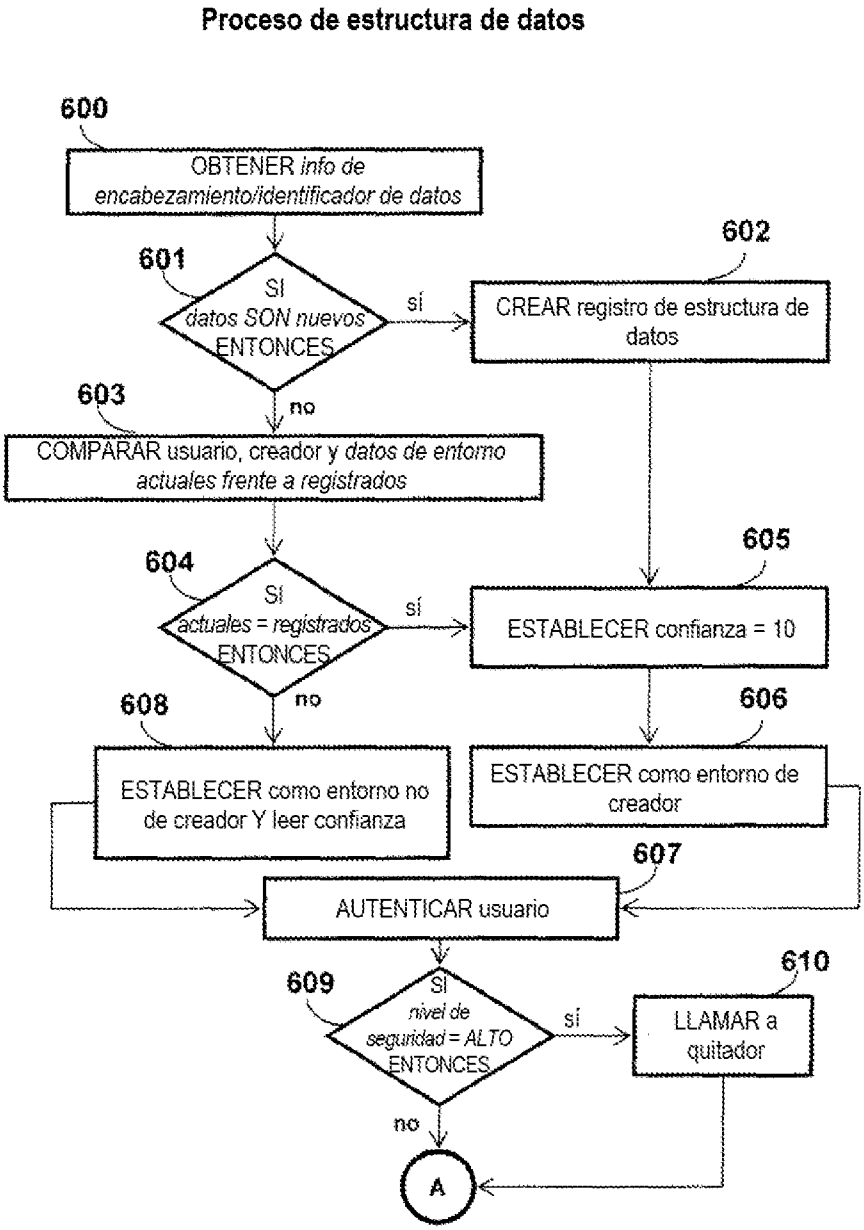
Proceso de estructura de datos
600
OBTENER info de encabezamiento/identificador de datos
601
SI datos SON nuevos ENTONCES
sí
602
CREAR registro de estructura de datos
no
603
COMPARAR usuario, creador y datos de entorno actuales frente a registrados
604
SI actuales = registrados ENTONCES
sí
605
ESTABLECER confianza = 10
no
608
ESTABLECER como entorno no de creador Y leer confianza
606
ESTABLECER como entorno de creador
607
AUTENTICAR usuario
609
SI nivel de seguridad = ALTO ENTONCES
sí
610
LLAMAR a quitador
no
A

Fig. 6

Proceso de estructura de datos
continuación

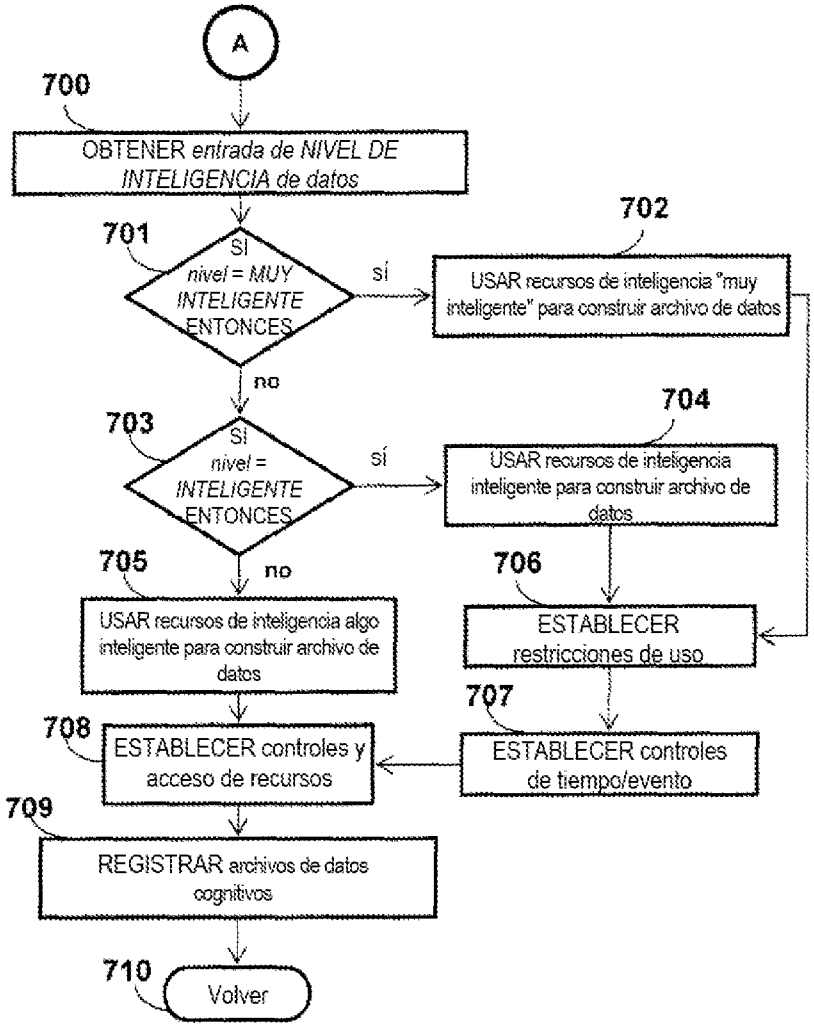

Fig. 7

Proceso quitador de procesador de datos cognitivos

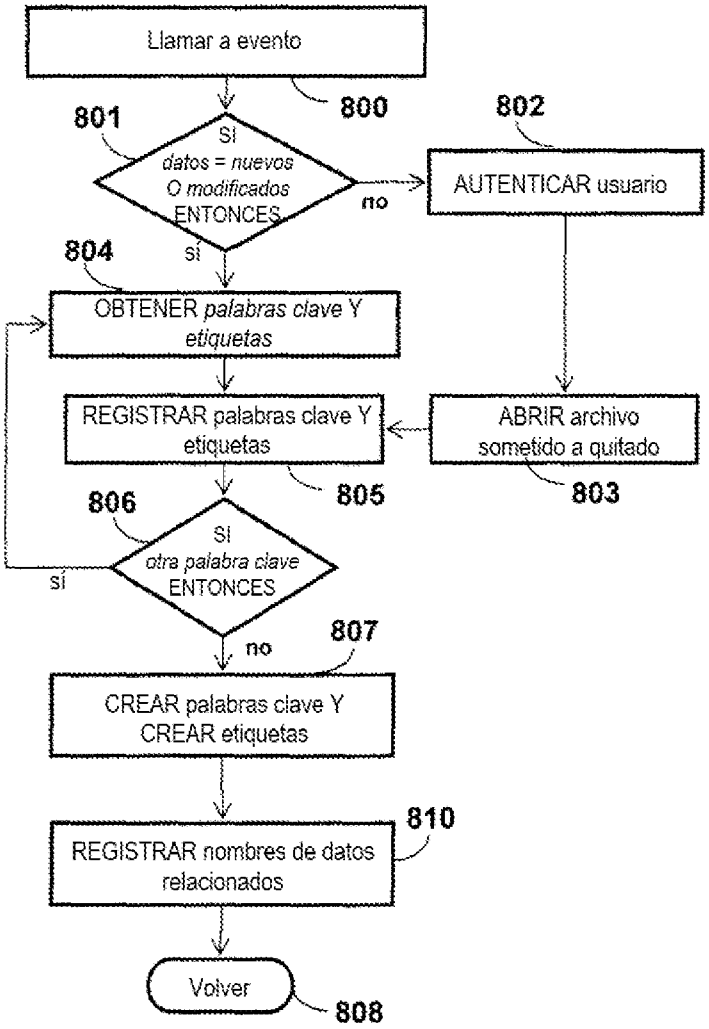

Fig. 8

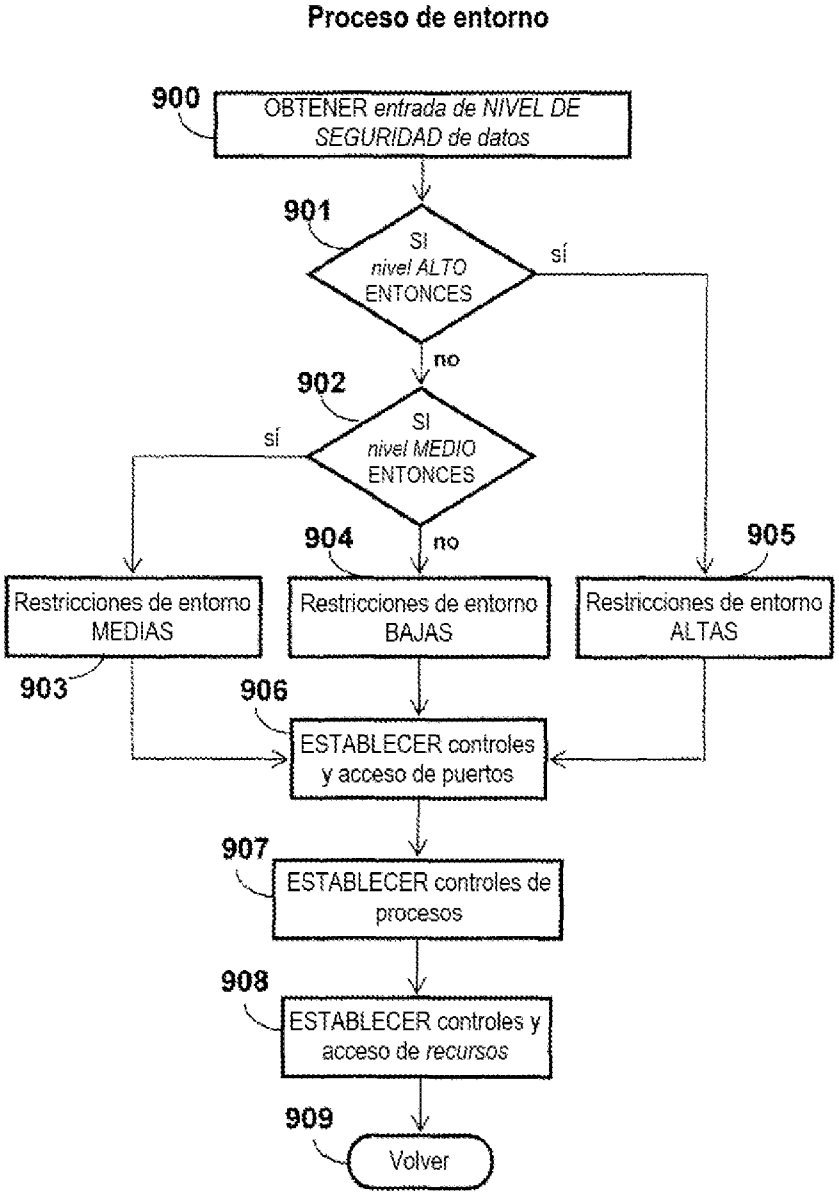
Proceso de entorno
900
OBTENER entrada de NIVEL DE SEGURIDAD de datos
901
SI nivel ALTO ENTONCES
sí
no
902
SI nivel MEDIO ENTONCES
sí
no
904
905
Restricciones de entorno MEDIAS
Restricciones de entorno BAJAS
Restricciones de entorno ALTAS
903
906
ESTABLECER controles y acceso de puertos
907
ESTABLECER controles de procesos
908
ESTABLECER controles y acceso de recursos
909
Volver

Fig. 9

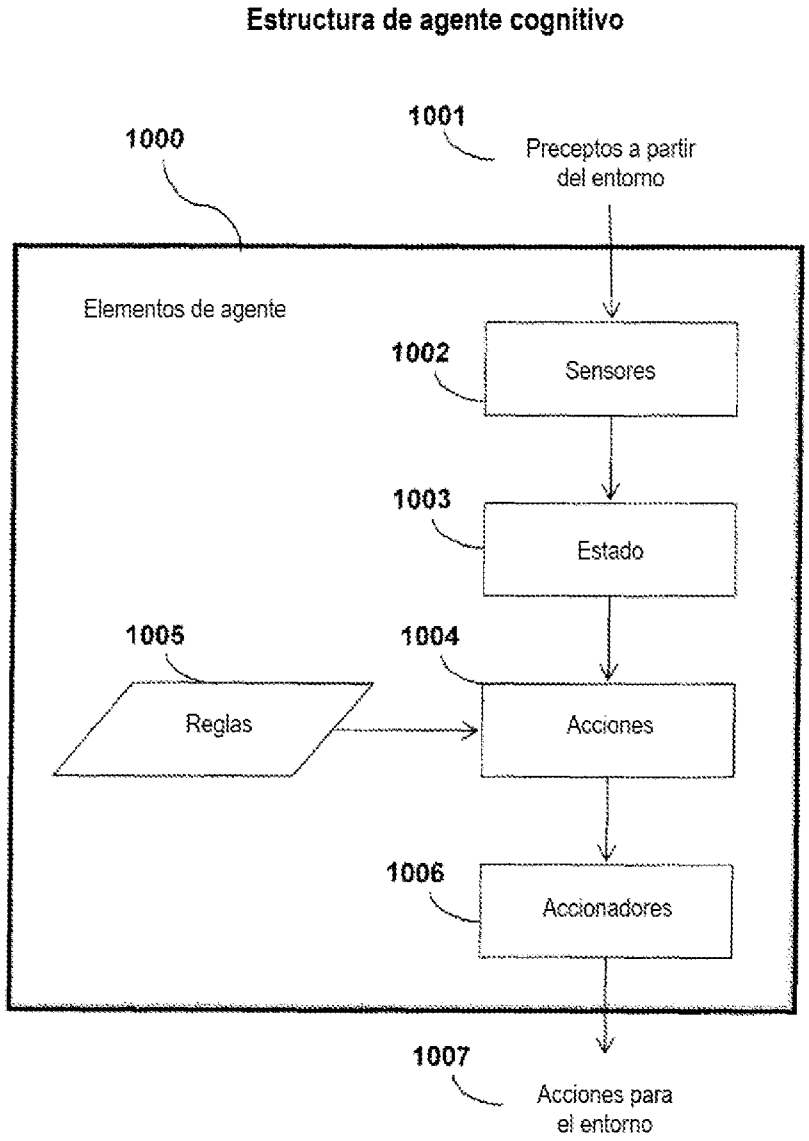
Estructura de agente cognitivo
1000
1001
Preceptos a partir del entorno
Elementos de agente
1002
Sensores
1003
Estado
1005
1004
Reglas
Acciones
1006
Accionadores
1007
Acciones para el entorno

Fig. 10

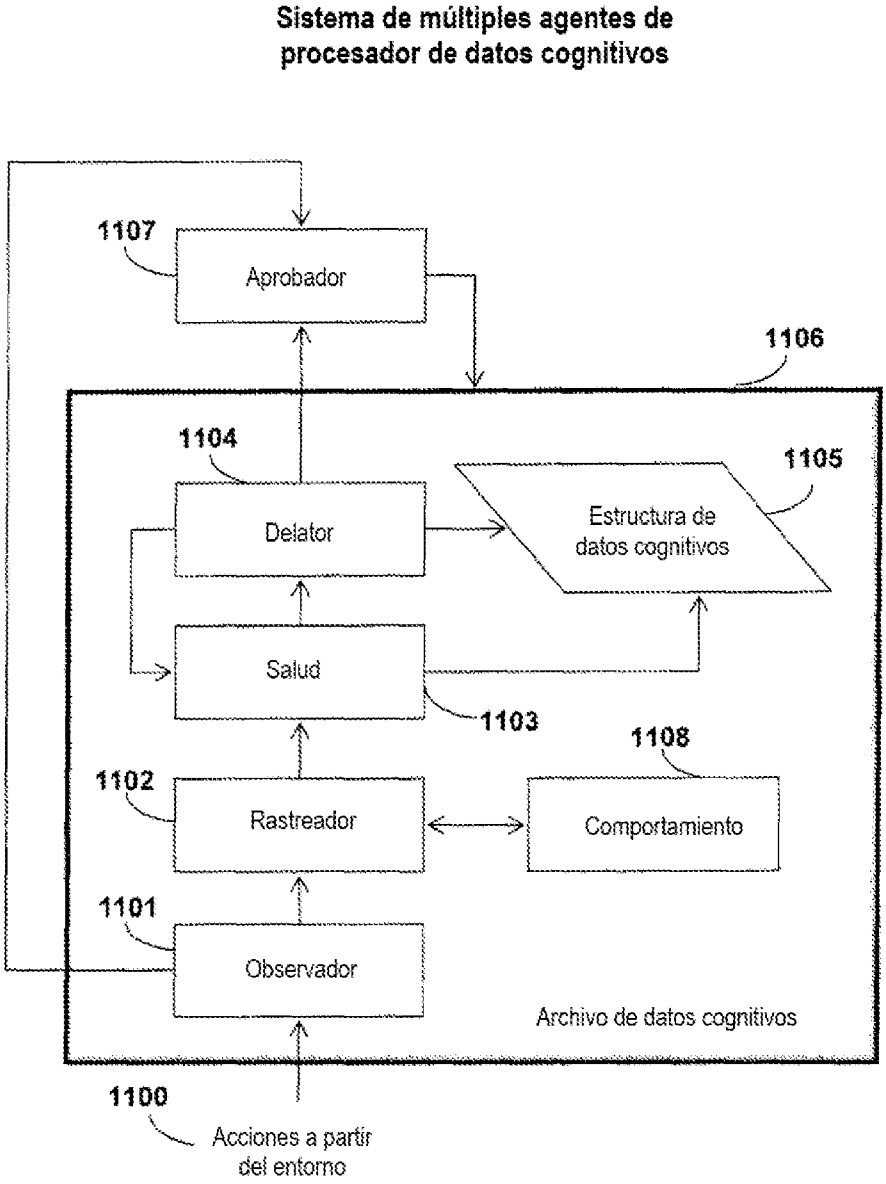
Sistema de múltiples agentes de procesador de datos cognitivos
1107
Aprobador
1106
1104
1105
Delator
Estructura de datos cognitivos
Salud
1103
1108
1102
Rastreador
Comportamiento
1101
Observador
Archivo de datos cognitivos
1100
Acciones a partir del entorno

Fig. 11

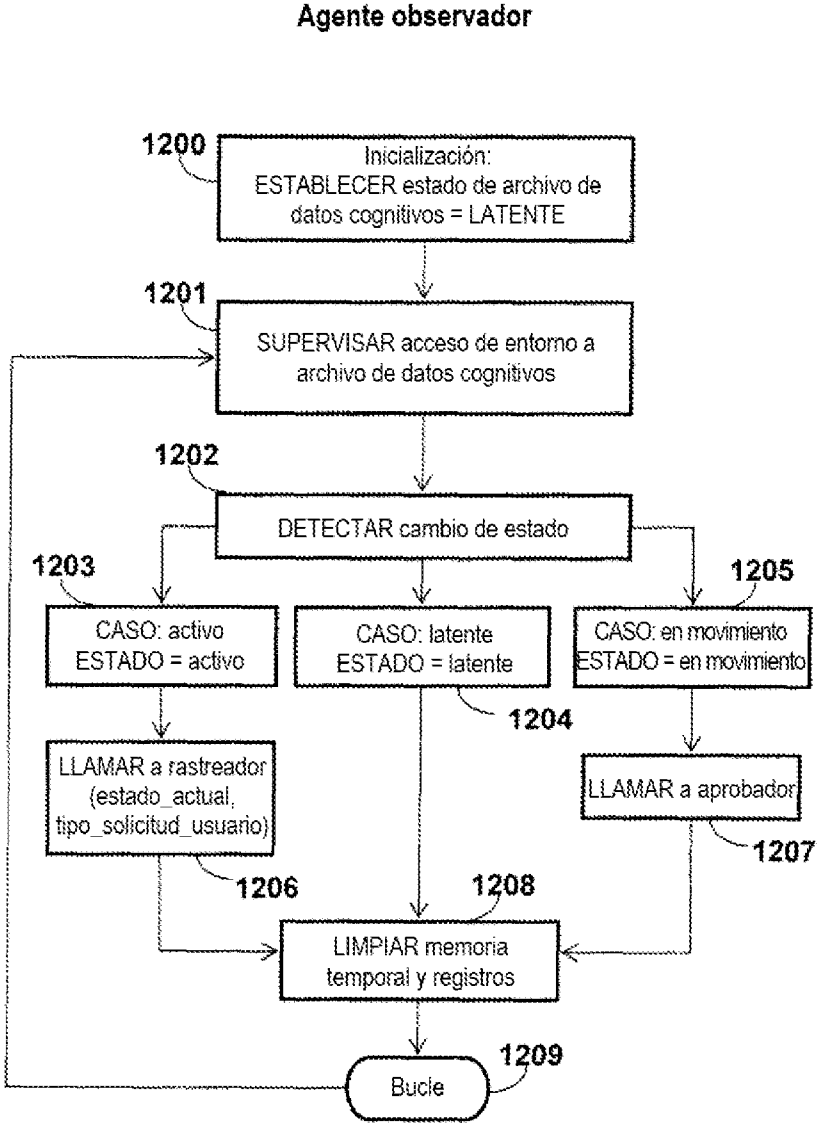
Agente observador
1200
Inicialización:
ESTABLECER estado de archivo de datos cognitivos = LATENTE
1201
SUPERVISAR acceso de entorno a archivo de datos cognitivos
1202
DETECTAR cambio de estado
1203
CASO: activo
ESTADO = activo
CASO: latente
ESTADO = latente
1204
1205
CASO: en movimiento
ESTADO = en movimiento
LLAMAR a rastreador (estado_actual, tipo_solicitud_usuario)
1206
LLAMAR a aprobador
1207
1208
LIMPIAR memoria temporal y registros
1209
Bucle

Fig. 12

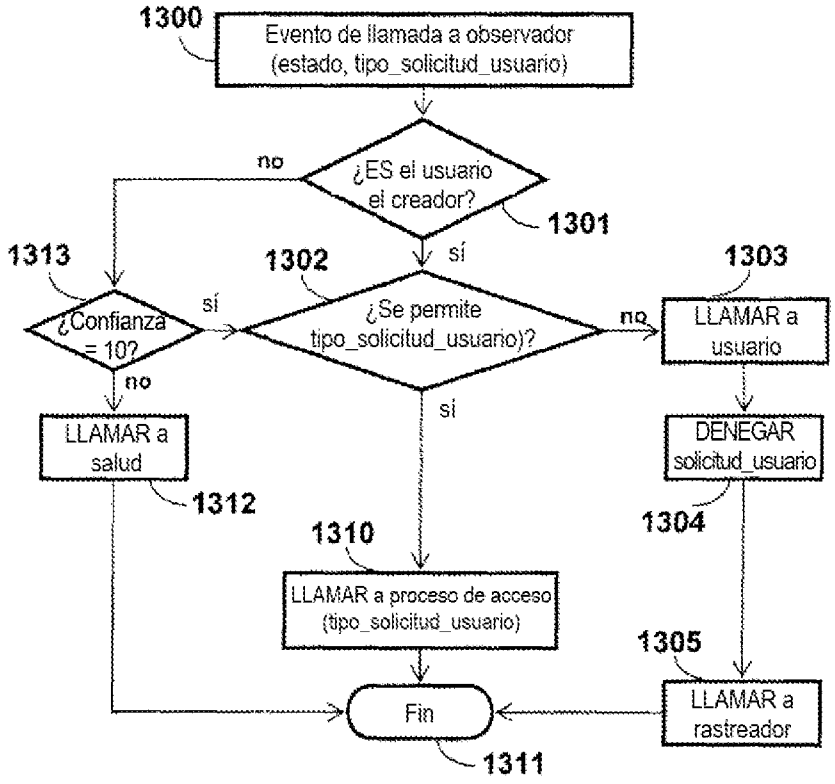
Precepto de observador de agente aprobador
1300
Evento de llamada a observador (estado, tipo_solicitud_usuario)
¿ES el usuario el creador?
1301
no
sí
1313
1302
1303
¿Confianza = 10?
sí
¿Se permite tipo_solicitud_usuario)?
no
LLAMAR a usuario
no
sí
LLAMAR a salud
1312
DENEGAR solicitud_usuario
1304
1310
LLAMAR a proceso de acceso (tipo_solicitud_usuario)
1305
Fin
LLAMAR a rastreador
1311

Fig. 13

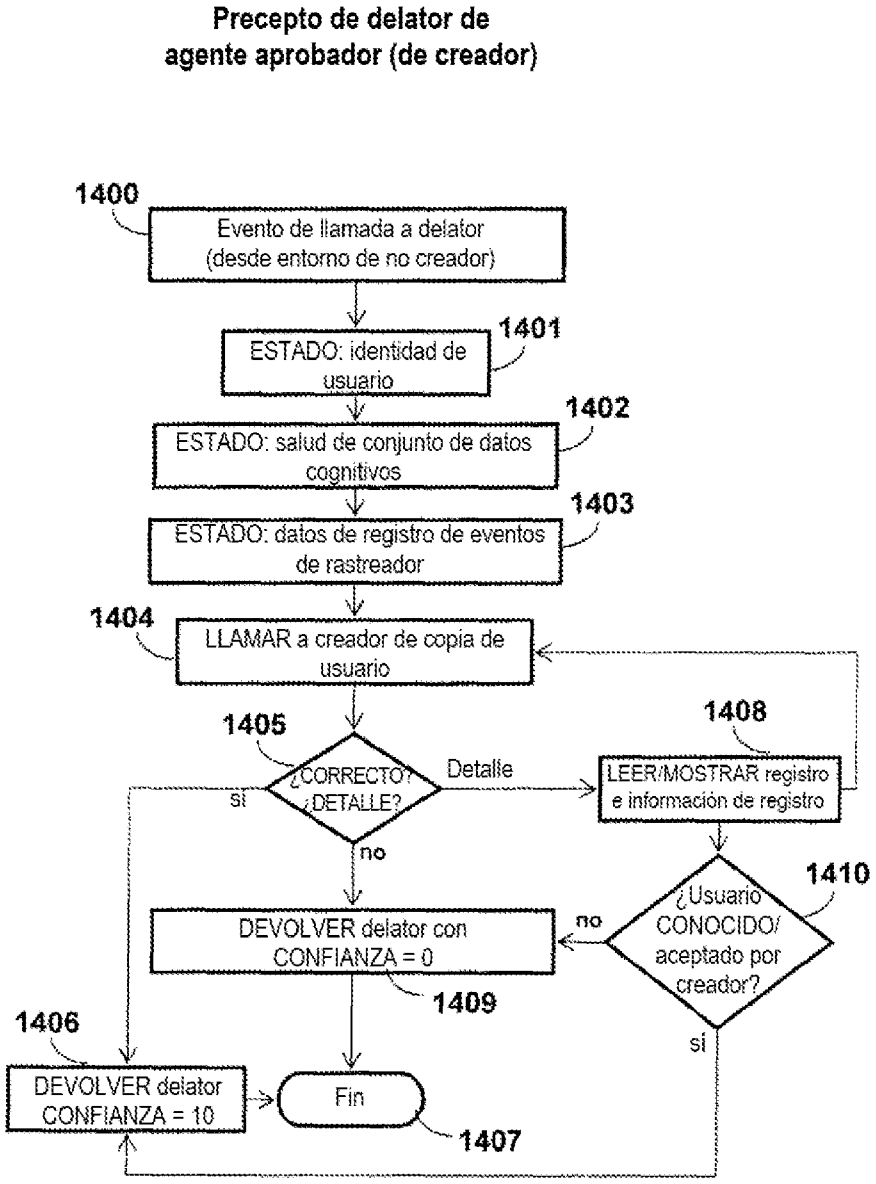
Precepto de delator de agente aprobador (de creador)
1400
Evento de llamada a delator (desde entorno de no creador)
1401
ESTADO: identidad de usuario
1402
ESTADO: salud de conjunto de datos cognitivos
1403
ESTADO: datos de registro de eventos de rastreador
1404
LLAMAR a creador de copia de usuario
1405
¿CORRECTO? ¿DETALLE?
Detalle
si
no
1408
LEER/MOSTRAR registro e información de registro
1410
¿Usuario CONOCIDO/ aceptado por creador?
no
si
DEVOLVER delator con CONFIANZA = 0
1409
1406
DEVOLVER delator CONFIANZA = 10
Fin
1407

Fig. 14

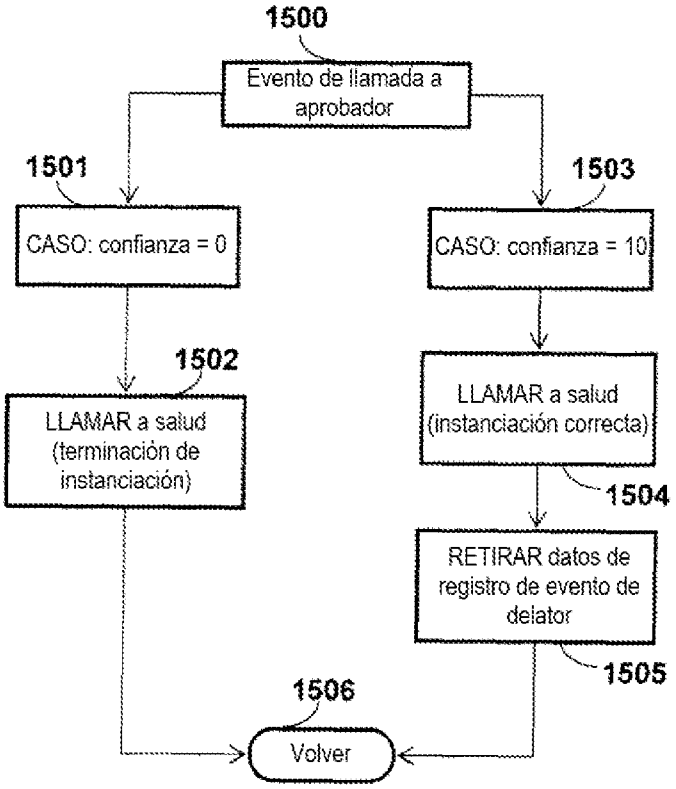
Precepto de aprobador de agente delator
1500
Evento de llamada a aprobador
1501
CASO: confianza = 0
1503
CASO: confianza = 10
1502
LLAMAR a salud (terminación de instanciación)
LLAMAR a salud (instanciación correcta)
1504
RETIRAR datos de registro de evento de delator
1505
1506
Volver

Fig. 15

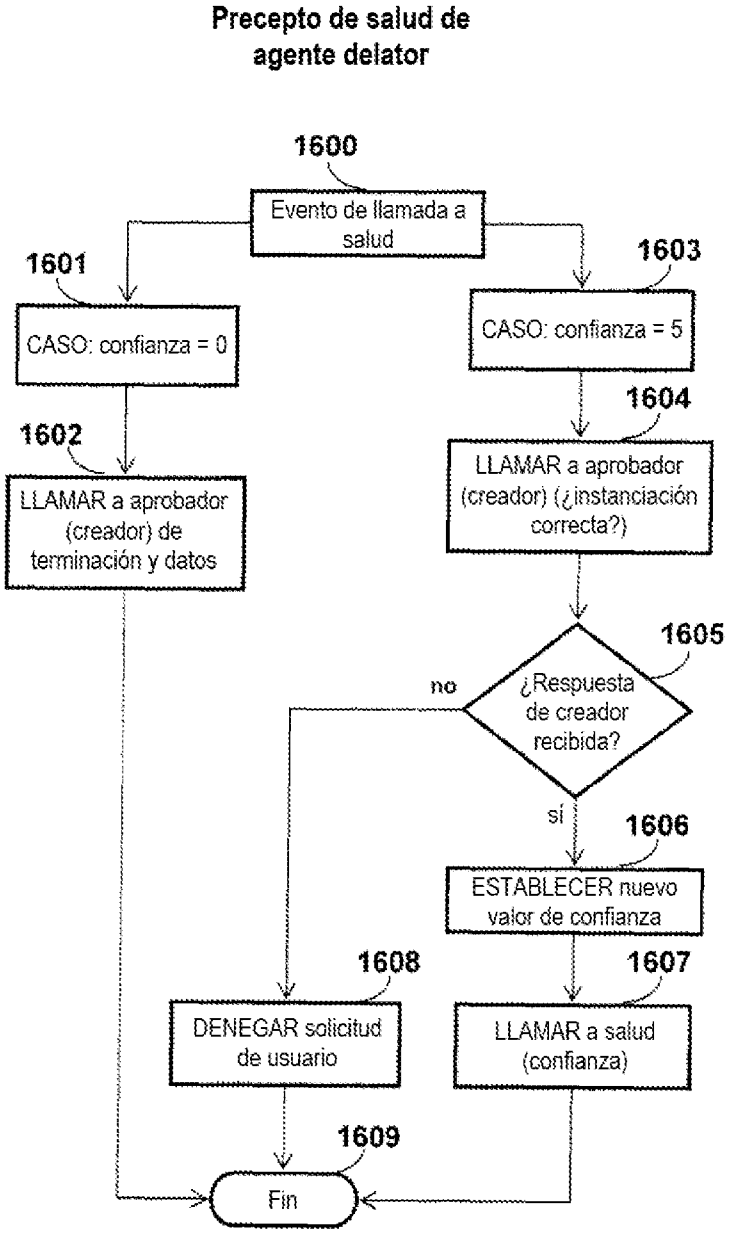
Precepto de salud de agente delator
1600
Evento de llamada a salud
1601
CASO: confianza = 0
1602
LLAMAR a aprobador (creador) de terminación y datos
1603
CASO: confianza = 5
1604
LLAMAR a aprobador (creador) (¿instanciación correcta?)
1605
¿Respuesta de creador recibida?
no
sí
1606
ESTABLECER nuevo valor de confianza
1607
LLAMAR a salud (confianza)
1608
DENEGAR solicitud de usuario
1609
Fin

Fig. 16

Preceptos de delator, aprobador y rastreador de agente de salud

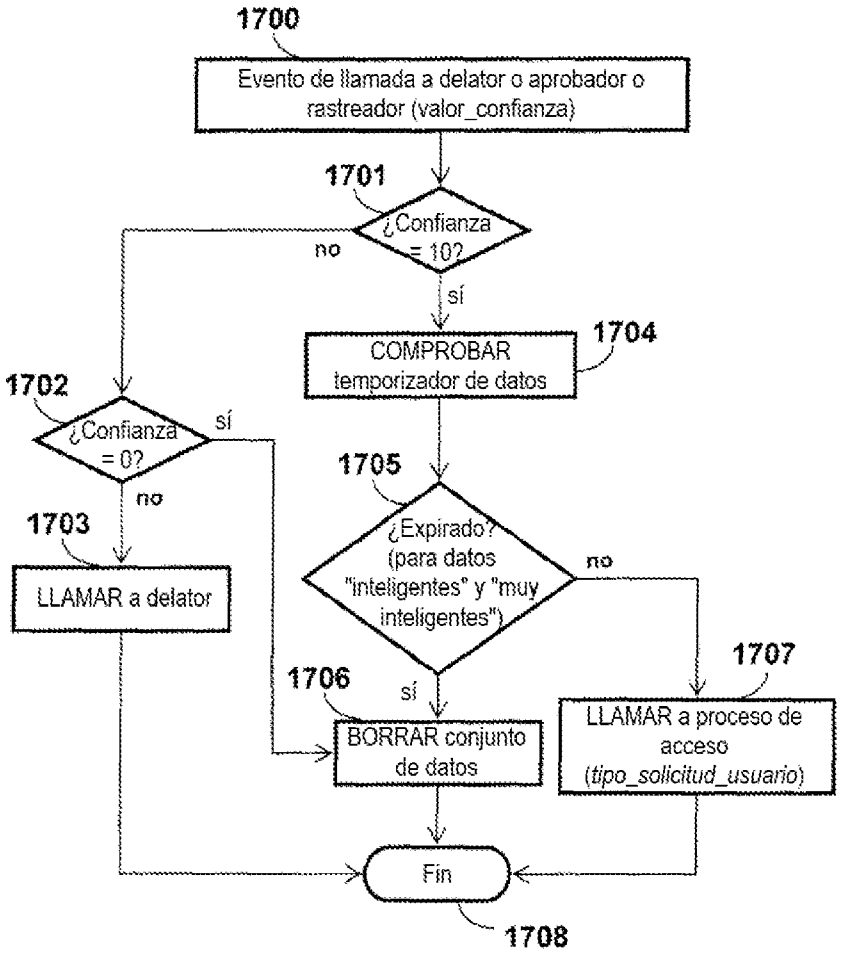

Fig. 17

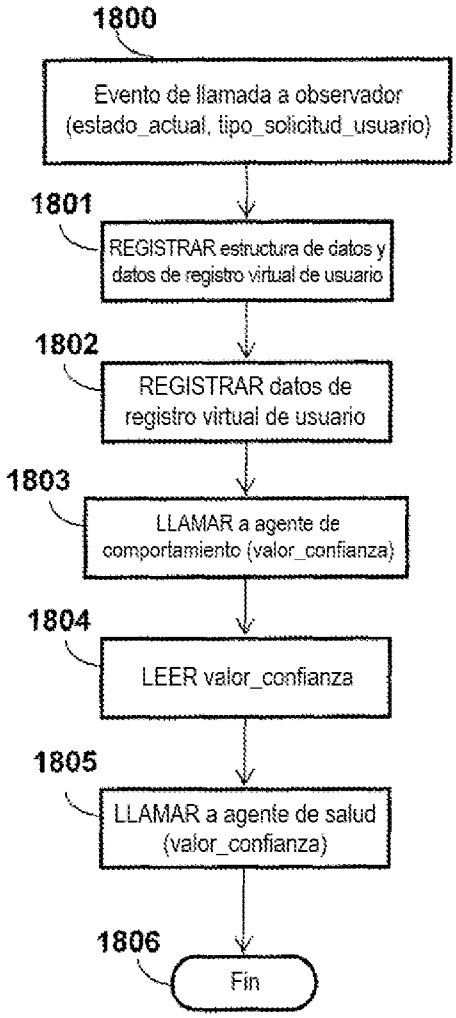
Precepto de observador de agente rastreador
1800
Evento de llamada a observador (estado_actual, tipo_solicitud_usuario)
1801
REGISTRAR estructura de datos y datos de registro virtual de usuario
1802
REGISTRAR datos de registro virtual de usuario
1803
LLAMAR a agente de comportamiento (valor_confianza)
1804
LEER valor_confianza
1805
LLAMAR a agente de salud (valor_confianza)
1806
Fin

Fig. 18

Agente de comportamiento
(empresa)

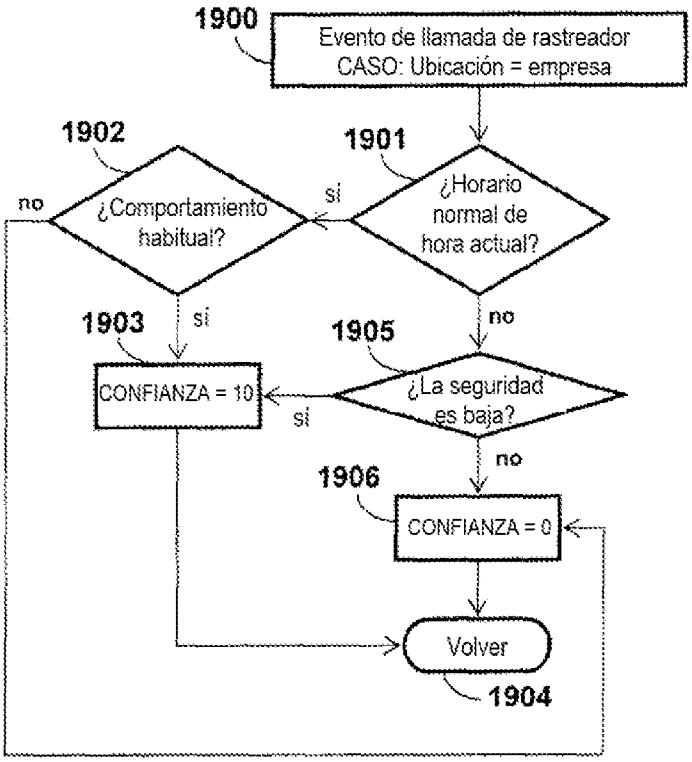

Fig. 19

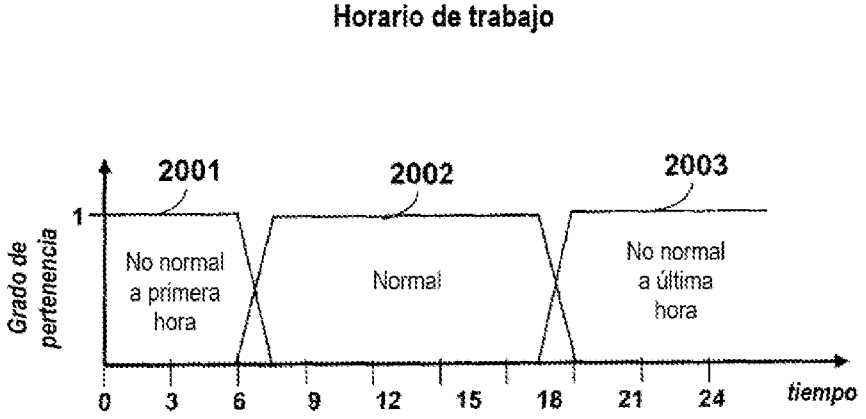
Horario de trabajo
2001
2002
2003
1
Grado de pertenencia
No normal a primera hora
Normal
No normal a última hora
0
3
6
9
12
15
18
21
24
tiempo

Fig. 20

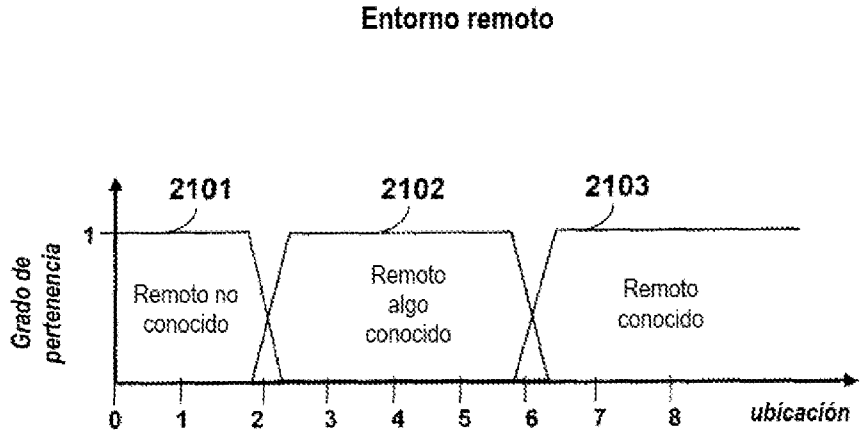
Entorno remoto
2101
2102
2103
1
Grado de pertenencia
Remoto no conocido
Remoto algo conocido
Remoto conocido
0
1
2
3
4
5
6
7
8
ubicación

Fig. 21

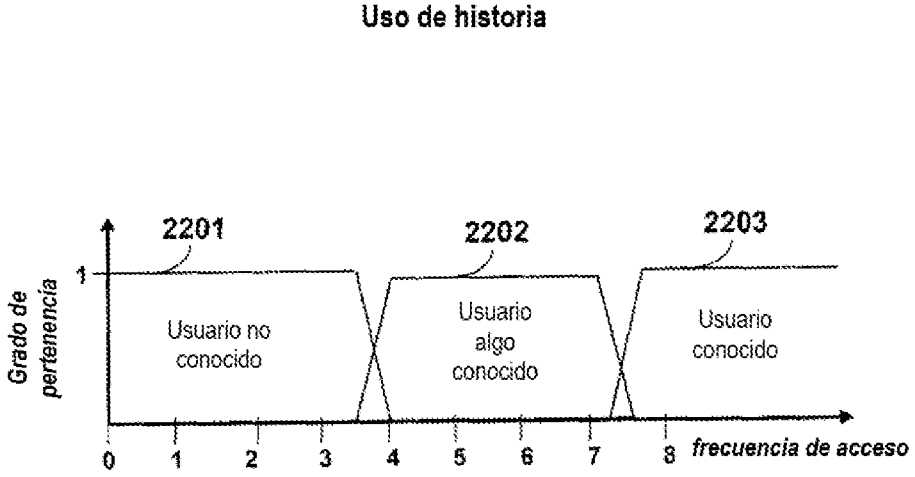
Uso de historia
2201
2202
2203
1
Grado de pertenencia
Usuario no conocido
Usuario algo conocido
Usuario conocido
0
1
2
3
4
5
6
7
8
frecuencia de acceso

Fig. 22

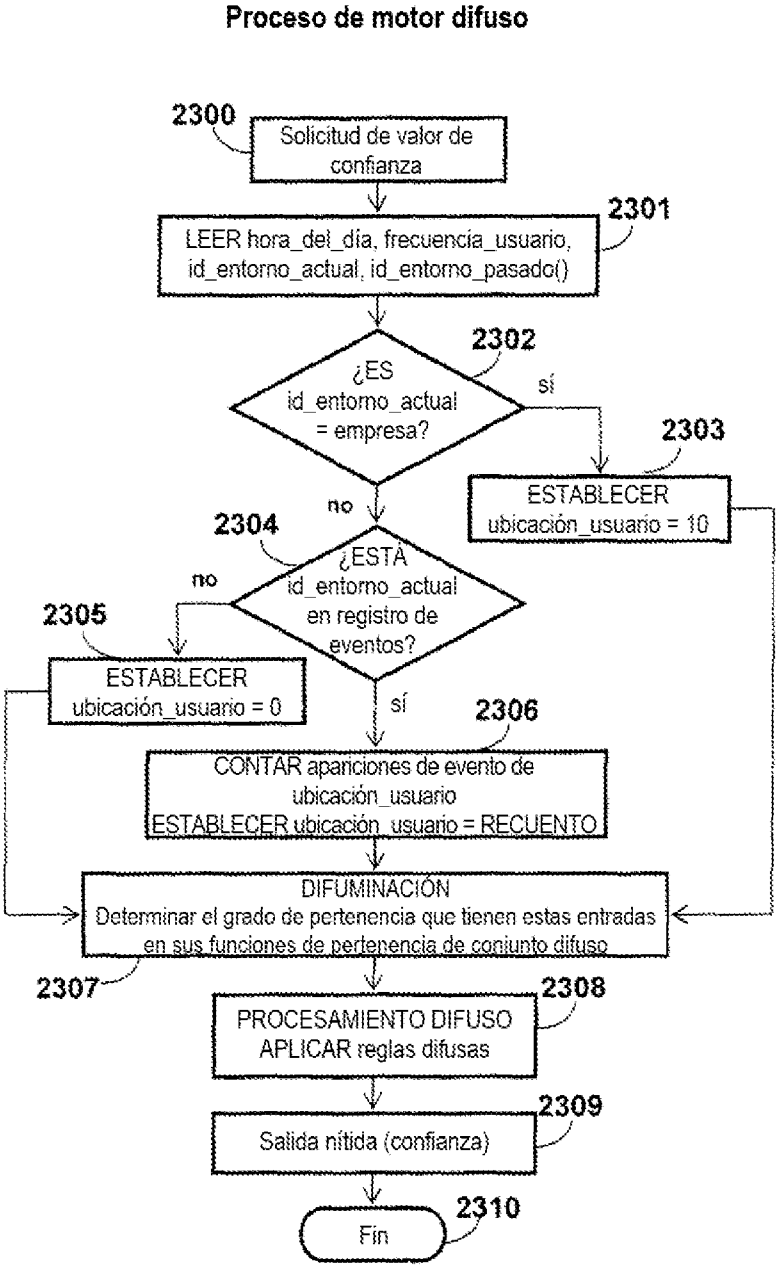
Proceso de motor difuso
2300
Solicitud de valor de confianza
2301
LEER hora_del_día, frecuencia_usuario, id_entorno_actual, id_entorno_pasado()
2302
¿ES id_entorno_actual = empresa?
sí
2303
ESTABLECER ubicación_usuario = 10
no
2304
¿ESTÁ id_entorno_actual en registro de eventos?
no
2305
ESTABLECER ubicación_usuario = 0
sí
2306
CONTAR apariciones de evento de ubicación_usuario
ESTABLECER ubicación_usuario = RECUENTO
DIFUMINACIÓN
Determinar el grado de pertenencia que tienen estas entradas en sus funciones de pertenencia de conjunto difuso
2307
2308
PROCESAMIENTO DIFUSO
APLICAR reglas difusas
2309
Salida nítida (confianza)
2310
Fin

Fig. 23

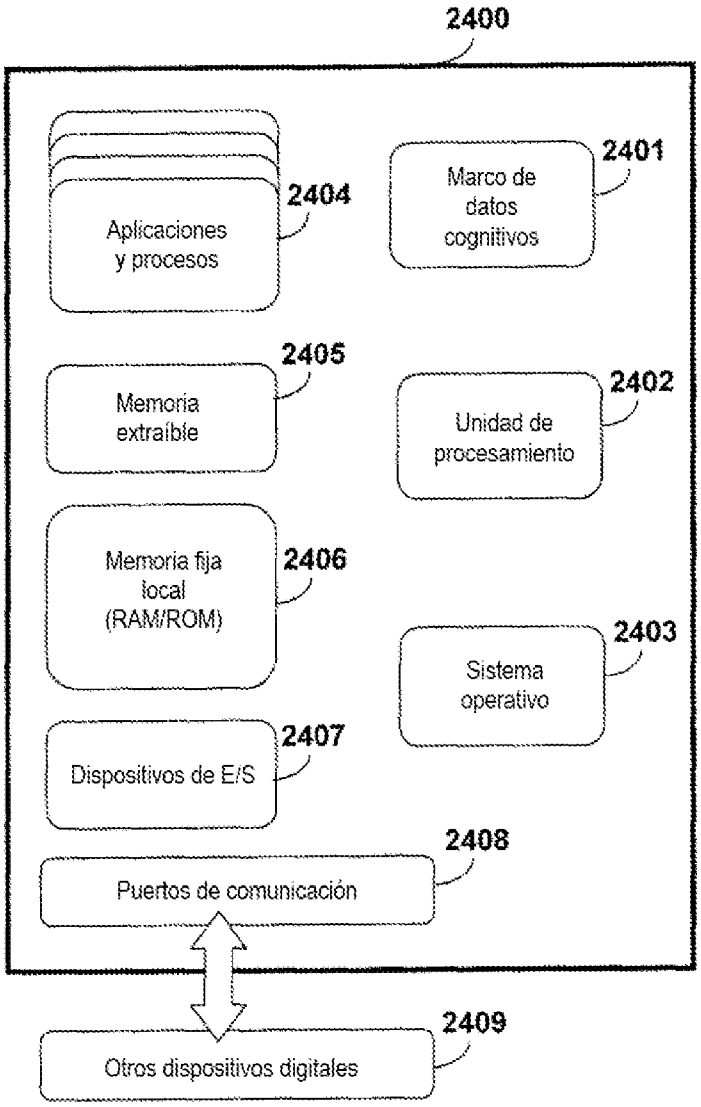
2400
Aplicaciones y procesos
2404
Marco de datos cognitivos
2401
Memoria extraíble
2405
Unidad de procesamiento
2402
Memoria fija local (RAM/ROM)
2406
Sistema operativo
2403
Dispositivos de E/S
2407
Puertos de comunicación
2408
Otros dispositivos digitales
2409

Fig. 24