

19



OFICINA ESPAÑOLA DE  
PATENTES Y MARCAS

ESPAÑA



11 Número de publicación: **2 634 822**

51 Int. Cl.:

**G08B 25/14** (2006.01)

**G08B 29/16** (2006.01)

12

TRADUCCIÓN DE PATENTE EUROPEA

T3

96 Fecha de presentación y número de la solicitud europea: **07.01.2013 E 13150435 (9)**

97 Fecha y número de publicación de la concesión europea: **21.06.2017 EP 2615593**

54 Título: **Almacenamiento de sistema de seguridad de datos persistentes**

30 Prioridad:

**11.01.2012 US 201213348187**

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

**29.09.2017**

73 Titular/es:

**HONEYWELL INTERNATIONAL INC. (100.0%)  
115 Tabor Road  
Morris Plains, NJ 07950, US**

72 Inventor/es:

**STANTON, DOUGAL;  
PROBIN, ROBERT JOHN;  
CRISP, MARTIN;  
OSBORNE, KENNETH y  
MCWHIRTER, ALAN ROBERT**

74 Agente/Representante:

**LEHMANN NOVO, María Isabel**

**ES 2 634 822 T3**

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**

Almacenamiento de sistema de seguridad de datos persistentes

5 **CAMPO DE LA INVENCION**

La presente solicitud de patente se refiere a un sistema de seguridad, y más en particular, a un sistema de seguridad y un método para controlar a distancia una o más áreas especificadas.

10 **ANTECEDENTES DE LA INVENCION**

Los sistemas de seguridad típicos, actualmente conocidos, suelen incluir un dispositivo de control in situ tal como un panel de control. El panel de control puede incluir un microprocesador con software o firmware preparados para controlar uno o más sensores designados para áreas especificadas. Los sensores pueden dividirse en zonas de seguridad que son todas ellas controladas por el panel de control central. El panel de control es un coste importante del sistema de seguridad. El sistema de seguridad, que incluye el panel de control, requiere actividades de instalación, inspecciones, mantenimiento, reparaciones y actualizaciones. El hardware del panel de control puede ser de alto coste y la instalación requiere el tiempo de dedicación de un técnico especializado. Además, cuando se actualiza el software o el firmware, un técnico tiene que visitar la instalación en donde está situado el sistema de seguridad y el panel de control, lo que resulta costoso y consumidor de tiempo. Además, es posible que la actualización del sistema de seguridad requiera equipos físicos adicionales o cambiarlos para permitir la activación de nuevas características o funciones, lo que puede ser costoso y requerir el tiempo de un técnico especializado. Además, un proveedor y/o almacén pueden tener que almacenar grandes cantidades de diversos tipos de paneles para satisfacer la demanda, con el coste consiguiente.

En numerosos tales sistemas de seguridad, se ha requerido un almacenamiento persistente, con tales requisitos satisfechos por sistemas de memoria RAM alimentados por baterías o dispositivos de memoria EEPROM. Sin embargo, a medida que se han desarrollado las exigencias de memoria/almacenamiento para dichos sistemas, tales sistemas han utilizado, cada vez más, sistemas de almacenamiento IC instantáneos. Aunque los sistemas de almacenamiento IC instantáneos proporcionan más capacidad de almacenamiento por unidad de coste, están más limitados que los sistemas de memoria y los dispositivos de memoria EEPROM. De este modo, aunque los sistemas de memoria RAM salvaguardarán, casi instantáneamente, datos en un número ilimitado de veces y los dispositivos de memoria EEPROM (aunque más lentos que los sistemas de memoria RAM) son capaces de realizar la escritura de millones de bytes individuales o palabras por célula de memoria, los sistemas de memorización instantánea ventajosamente con un menor coste relativo son todavía más lentos (tardando más en las funciones de borrado y escritura). Además, los sistemas de memorización instantánea tienen una vida útil limitada susceptible de escritura y requieren que los datos sean borrados y objeto de escritura en grandes bloques o páginas. En consecuencia, con el fin de utilizar dichos sistemas de memorización instantánea en sistemas de seguridad, se hizo necesaria una gestión compleja para el tratamiento y escritura de datos, de forma eficiente, para ser capaces de minimizar los ciclos de lectura/escritura que tienen lugar durante el funcionamiento normal del sistema de seguridad.

La publicación de patente de los Estados Unidos nº US 2009/0322527 A1 (titulada "Sistema de seguridad distribuido basado en servidor", publicada con fecha 31 de diciembre de 2009) da a conocer un sistema que puede utilizarse para gestionar los requisitos de memoria de los sistemas de seguridad.

El documento EP 2 284 816 A1 da a conocer un método de almacenar datos persistentes para un sistema de seguridad que tiene un panel de control local en comunicación con un servidor distante, teniendo dicho panel de control local un almacenamiento de datos local, y teniendo dicho servidor distante un almacenamiento distante de dicho almacenamiento de datos local, incluyendo la etapa de salvaguardar periódicamente partes lógicas de datos persistentes existentes en el servidor distante.

La idea inventiva presente está destinada a proporcionar los requisitos de memoria y almacenamiento de datos de un sistema de seguridad en donde se puede maximizar la vida útil del hardware.

55 **SUMARIO DE LA INVENCION**

En un aspecto de la presente solicitud de patente, se da a conocer un método para el almacenamiento de datos persistentes para un sistema de seguridad que tiene un panel de control local en comunicación con un servidor distante, en donde el panel de control local tiene un almacenamiento de datos local y el servidor distante tiene un almacenamiento distante desde el almacenamiento de datos local. El método incluye las etapas de (1) salvaguardar periódicamente partes lógicas de datos persistentes existentes en el servidor distante, (2) salvaguardar periódicamente las partes lógicas de datos persistentes existentes en el almacenamiento de datos local, en donde las partes lógicas de los datos persistentes existentes incluye, cada una de ellas, un elemento de datos de distinción, (3) salvaguardar el elemento de datos de distinción en el almacenamiento de datos local de cada parte lógica del datos persistentes existentes salvaguardados solamente en el servidor distante; y (4) reconstruir los datos persistentes en el panel de control local después de reiniciar operativamente el panel de control local. La

5 salvaguarda periódica en el almacenamiento de datos local se realiza con menos frecuencia que la salvaguarda periódica en el servidor distante. Durante la etapa de reconstrucción, solamente las partes lógicas de datos persistentes existentes, que tienen elementos de datos de distinción posteriores al elemento de datos de distinción salvaguardado en el almacenamiento de datos local, son objeto de escritura desde el almacenamiento distante y salvaguardados en el almacenamiento de datos local.

En una forma de este aspecto de la idea inventiva, los elementos de datos de distinción, son marcas temporales.

10 En otra forma de este aspecto de la idea inventiva, el almacenamiento de datos local es una memoria no volátil. En una forma adicional, el almacenamiento de datos local es una memoria instantánea.

15 En otra forma de este aspecto de la idea inventiva, el almacenamiento de datos distante es al menos un dispositivo de entre los dispositivos de memoria RAM y de memoria EEPROM. En otra forma adicional, el almacenamiento de datos local es una memoria instantánea.

20 En otro aspecto de la idea inventiva, se da a conocer un sistema de seguridad, que incluye dispositivos de seguridad que generan datos persistentes, un sistema de control local que recibe los datos persistentes desde los dispositivos de seguridad, incluyendo el sistema de control local, un microprocesador y una memoria no volátil, y un servidor distante desde el sistema de control local. El servidor distante tiene un almacenamiento de datos distante y está en comunicación con el microprocesador del sistema de control local. El microprocesador transmite periódicamente partes lógicas de los datos persistentes existentes al servidor distante para su salvaguarda en el almacenamiento de datos distantes, en donde las partes lógicas de datos persistentes existentes, incluyen, cada una de ellas, un elemento de datos de distinción. El microprocesador salvaguarda periódicamente, además, las partes lógicas de datos persistentes existentes en la memoria no volátil del sistema de control local, con menos frecuencia que se salvaguardan periódicamente los datos persistentes en el almacenamiento de datos distante, y salvaguarda el elemento de datos de distinción en el almacenamiento de datos local para cada parte lógica de datos persistentes existentes salvaguardados solamente en el servidor distante. Cuando se reinicia operativamente el sistema de control local, el microprocesador recupera, desde el almacenamiento de datos distante, solamente las partes lógicas de datos persistentes existentes que tienen elementos de datos de distinción posteriores al elemento de datos de distinción salvaguardado en la memoria no volátil del sistema de control de datos local.

30 En una forma de realización de este aspecto, los elementos de datos de distinción son marcas temporales.

35 En otra forma de este aspecto de la idea inventiva, la memoria no volátil comprende una memorización instantánea de IC.

40 En otra forma de este aspecto de la idea inventiva, el almacenamiento de datos distante es al menos uno de entre dispositivos de memoria RAM y de memoria EEPROM. En una forma adicional, la memoria no volátil es una memoria IC instantánea.

Otras características y ventajas se harán evidentes a partir de una revisión de la especificación completa, incluyendo las reivindicaciones y los dibujos adjuntos.

#### 45 BREVE DESCRIPCIÓN DE LOS DIBUJOS

La Figura es una vista esquemática de un sistema de seguridad en conformidad con la presente invención.

#### DESCRIPCIÓN DETALLADA DE LA INVENCION

50 Un sistema de seguridad 10 de conformidad con la presente solicitud de patente se ilustra en la Figura. El sistema de seguridad 10 incluye un sistema de control local 20 (p.ej., un panel de control) que incluye un microprocesador/microcontrolador 22 y una memoria no volátil 26.

55 Como debe apreciarse cuando se tiene un conocimiento completo de la presente invención, la memoria no volátil 26 puede ser ventajosamente, a modo de ejemplo, dispositivos de memorización instantánea de coste relativamente bajo, aun cuando dichos dispositivos suelen ser más lentos, tengan una vida útil, susceptible de escritura, más limitada, y requieran una gestión más compleja, que otros dispositivos de memoria (de mayor coste). Los ahorros de costes de la utilización y preservación, una memoria no volátil de bajo coste 26 se hace cada vez más valiosa a medida que siguen aumentando las necesidades de memoria de los sistemas de seguridad 10.

60 El microprocesador 22 está en comunicación mediante enlaces de datos 30 (que pueden ser cualquier enlace de comunicaciones adecuado, cableado o inalámbrico) a otros dispositivos del sistema de seguridad 40, 42 tales como alarmas, monitores de estados operativos, detectores de movimientos, etc.

65 El microprocesador está también en comunicación mediante enlaces de datos 50 (que pueden ser también cualquier enlace de comunicaciones adecuado para transmitir datos) a un servidor distante 60 que está enlazado con el

almacenamiento de datos distante 70.

Los enlaces de datos 50 pueden, ventajosamente, tener una conexión de datos 'siempre activa' a un servidor distante, lo que permite al servidor distante 60 ejecutar, también ventajosamente, un programa informático para salvaguardar la configuración del panel de alarma y enviar esta configuración a, por ejemplo, un panel de alarma. Sin embargo, debe apreciarse que la conexión mediante enlaces de datos 50 podría ser, como alternativa, una conexión de datos 'bajo demanda' (p.ej., 'marcación' de red PSTN) y/o los datos podrían memorizarse y enviarse periódicamente mediante una conexión periódica o menos que una conexión 'bajo demanda'. Si se utilizan enlaces de datos 'bajo demanda' 50, los enlaces 50 pueden tener, ventajosamente, un tiempo de conexión bajo con el fin de no cargar potencialmente el sistema de control local 20 con una memoria caché/intermedia de datos local.

Además, debe apreciarse que una señal 'mantenida activa' o 'operativamente sensible', entre el sistema de control local 20 y el servidor distante 60, podría proporcionarse ventajosamente en la operación, en donde una anomalía se señalaría a un centro de recepción de alarmas (supervisión) si no está disponible la comunicación de datos a través de los enlaces 50.

Debe apreciarse también que los enlaces de datos 50 pueden ser de "señalización de ruta dual" o de señalización de múltiples rutas con el fin de aumentar la solidez de la conexión de datos al servidor distante 60. Además, tipos de conexión podrían mezclarse dentro del alcance de la presente invención con, a modo de ejemplo, una ruta de comunicación primaria "siempre activa" con conexiones secundarias y terciarias que sean conexiones "bajo demanda". Por supuesto, métodos de encriptación y autenticación adecuados pueden utilizarse también, ventajosamente, con las comunicaciones de datos a través de los enlaces de datos 50 por razones de seguridad.

El almacenamiento de datos distante 70 puede ser unidades de disco duro de PC o ventajosamente, a modo de ejemplo, sistemas de memoria RAM con alimentación de baterías (que permiten salvaguardar casi instantáneamente escrituras ilimitadas) o dispositivos de memoria EEPROM (que permiten millones de escritura por célula de memoria, y dichas escrituras pueden ser por byte individual o palabra). Además, debe apreciarse que, de conformidad con la presente invención, el almacenamiento de datos distante 70 podría realizarse, ventajosamente, mediante, a modo de ejemplo, un PC de servidor (bien sea en un lugar físicamente distante, bien sea en el emplazamiento local – para grandes instalaciones que tienen varios sistemas) pero no próximos al sistema de control real, una serie de PCs de servidor que comparten la carga útil (p.ej., un parque de servidores), que procesan el almacenamiento realizado mediante la denominada nube informática o una máquina dedicada que proporcione los servicios de almacenamiento.

El funcionamiento ventajoso del sistema de seguridad 10 de la presente invención es como sigue.

Los dispositivos del sistema de seguridad 40, 42 proporcionan datos incluyendo eventos (y registros de los eventos), datos en tiempo de ejecución (tal como estado operativo establecido/activado) y actualizaciones de datos de configuraciones de sistemas (todo ello referido, a continuación, como "datos persistentes") para el sistema de control local 20.

El microprocesador 22 envía datos persistentes recibidos existentes (en su integridad o en partes lógicas o en divisiones de los datos) directamente al servidor distante 60 por intermedio del enlace de datos 50, en donde los datos persistentes son objeto de escritura y salvaguardados en el almacenamiento de datos distante 70.

El microprocesador 22 causa también que los datos persistentes sean objeto de escritura periódica y se salvaguarden localmente en la memoria no volátil 26. Sin embargo, de conformidad con la presente invención, dichos datos persistentes se salvaguardan en la memoria no volátil local 26 con menos frecuencia que se salvaguardan en el almacenamiento de datos distante 70. Siempre que se realiza un almacenamiento menos frecuente de datos persistentes en la memoria no volátil local 26, el microprocesador 22 salvaguarda un elemento de datos que distingue que datos persistentes salvaguardados con respecto a otros datos persistentes (p.ej., una marca temporal, o números de índice secuenciales, incluyendo números de índices separados para subsistemas diferentes) y envía ese elemento de datos de distinción también al almacenamiento de datos distante 70.

Debe apreciarse, sin embargo, que pueden ser deseables variantes del almacenamiento anteriormente descrito en el sistema de control local 20. A modo de ejemplo, cuando se detectan eventos que indican un posible problema o el cese del funcionamiento normal (p.ej., la comunicación a través de los enlaces de datos 50 no está disponible, el sistema detecta el uso indebido, se produce una pérdida de potencia, se produce un fallo de batería o pérdida de batería, se recibe una orden de desactivación por el personal de servicio autorizado y/o el sistema 10 reconoce que se desactivará en un breve período de tiempo), los datos persistentes pueden salvaguardarse en la memoria no volátil 26 del sistema de control local y no quedarse a la espera de la siguiente escritura periódica planificada.

Cuando se reinicia operativamente el sistema de control local 20, según se realiza de vez en cuando, el microprocesador 22 actualiza su memoria no volátil local 26 sincronizando su último elemento de datos de distinción conocido con el servidor distante 60. Es decir, durante dicho proceso de reiniciación operativa, el microprocesador 22 determina si el almacenamiento de datos distante 70 tiene más recientes datos persistentes que se incluyen en la

5 memoria no volátil local 26. Si existen cualesquiera datos persistentes más recientes en el almacenamiento de datos distante 70, el servidor distante 60 comunica solamente esos datos persistentes más recientes, a través del enlace de comunicación 50, al sistema de control local 20 para almacenamiento de esos datos más recientes en la memoria no volátil local 26, lo que lleva al sistema de control local 20 a actualizarse para un funcionamiento continuado según se describió con anterioridad.

Además, debe apreciarse que datos extras que no se mantienen normalmente en el panel pueden utilizar este sistema 10 para ampliar la disponibilidad de memoria no volátil 26 en el sistema de control local 20.

10 De este modo, debe apreciarse que los sistemas de seguridad 10 configurados y en funcionamiento de conformidad con la presente invención reducirán la frecuencia de escritura de datos persistentes para la memoria no volátil 26 (p.ej., dispositivos de memoria instantánea), que aumentarán la vida útil de esa memoria. Además, dicha operación, memorizando los datos persistentes siempre en el almacenamiento de datos distante 70 puede evitar retardos en el tiempo de escritura tales como los que se producen con los dispositivos de memorización instantánea en el sistema  
15 de control local 20, y de modo similar, evita tiempos de borrado de circuito integrado (que pueden ser problemáticos) y reduce la necesidad de gestión instantánea compleja (reduciendo el uso de la memoria instantánea local 26). Todo lo que antecede puede reducir posiblemente el coste de paneles de control local 20 puesto que requieren menos memoria local.

20 Debe apreciarse también que el almacenamiento completo de datos persistentes en el almacenamiento de datos distante 70, según la presente invención, aumentará la seguridad de los datos claves (p.ej., la destrucción del sistema de control local no eliminará el registro de eventos completo), así como reducirá potencialmente la magnitud de almacenamiento de eventos requerido a nivel local, mientras que sigue manteniendo accesible los datos persistentes. Además, el personal de servicio autorizado obtiene acceso a los datos del registro de eventos desde el  
25 servidor distante 60, obviando la necesidad de entrar en contacto directo con el sistema de control local 20. Una ubicación distante es probable que tenga una conexión de más alto ancho de banda (y/o puede proporcionarse sin la necesidad o los gastos de proporcionar dichas conexiones de alta velocidad al sistema de control local 20), con lo que se reduce el tiempo y el coste de, a modo de ejemplo, una empresa de instalaciones para obtener acceso a esos datos. Además, dicha disponibilidad de datos permitirá, ventajosamente, que más datos estadísticos y otro análisis de datos de panel y otra información no anteriormente accesible sean fácilmente posible (p.ej., metodología de configuración del personal de instalación y eficiencia [a partir de la exploración de datos sobre ambos eventos y registros de información de marcas temporales de cambios de configuración de sistemas], con tendencias del registro de eventos para determinados tipos de eventos y establecer/omitir las tendencias de estados operativos).

35 Debe apreciarse, además, que los sistemas de seguridad 10, de conformidad con la presente invención, pueden tener acceso a una memoria considerablemente mayor (en el almacenamiento de datos distante 70) para una futura expansión, ampliamente sin límite. Como ya se indicó con anterioridad, dichos datos pueden todavía ser objeto de acceso por el sistema de control local 20, que proporciona acceso, a modo de ejemplo, a grandes cantidades de datos tales como datos de vídeo/imágenes y magnitud del registro de eventos.

40 Además, el sistema de seguridad 10 según aquí se da a conocer, añade redundancia a la configuración del sistema, datos de tiempo de ejecución y datos de registro de eventos puesto que normalmente los datos se memorizan en dos lugares: la memoria no volátil 26 del sistema de control local y el almacenamiento de datos distante 70 (además de cualquier copia de instalador, que es probable que esté sin actualizar desde hace meses). Dichas copias extras  
45 son mantenidas de forma fácil y a bajo coste, puesto que se realizan automáticamente durante el funcionamiento normal del sistema 10.

50 Asimismo, debe apreciarse que el sistema 10 según aquí se da a conocer, permite que datos extras que no sean críticos para el funcionamiento del sistema (y normalmente no estén salvaguardados a nivel local, debido a las limitaciones del almacenamiento local) sean salvaguardados a distancia y de forma segura en el almacenamiento de datos distante 70. Dichos datos útiles para el registro histórico y su analítica, pueden incluir, a modo de ejemplo, un registro histórico del estado de entrada de la fuente de alimentación de corriente alterna principal, niveles de tensión y cualesquiera picos de tensión, temperatura ambiente, estado de ventanas/puertas, calidad de comunicación 'bus-dispositivo' local cableada o inalámbrica, lecturas de resistencia de entrada ("Zona") y variantes y cambios de estado  
55 de marcas temporales, niveles de ruido local, niveles de luz ambiente, almacenamiento de imágenes para sistemas de entrada y supervisión de gas (p.ej., gas natural, CO<sub>2</sub>, O<sub>2</sub>).

60 Aunque una forma de realización y variantes han sido descritas en detalle con anterioridad, debe apreciarse que son todavía posibles otras modificaciones. A modo de ejemplo, los flujos lógicos ilustrados en la Figura no requieren el orden particular ilustrado, o un orden secuencial, para conseguir resultados deseables. Se pueden proporcionar otras etapas, o se pueden eliminar etapas, con respecto al flujo descrito, y se pueden añadir otros componentes o eliminarse de los sistemas descritos. Otras formas de realización pueden estar dentro del alcance de protección de las reivindicaciones siguientes.

65

**REIVINDICACIONES**

1. Un método de almacenamiento de datos persistentes para un sistema de seguridad (10) que tiene un panel de control local (20) en comunicación con un servidor distante (60), cuyo panel de control local (20) tiene un almacenamiento de datos local (26), y dicho servidor distante tiene un almacenamiento (70) distante de dicho almacenamiento de datos locales (26), que comprende las etapas de:
- 5 salvaguardar periódicamente partes lógicas de datos persistentes existentes a nivel del servidor distante (60),
- 10 salvaguardar periódicamente dichas partes lógicas de datos persistentes existentes a nivel de dicho almacenamiento de datos local (26),
- siendo dicha salvaguarda periódica a nivel de dicho almacenamiento de datos local (26) efectuada menos frecuentemente que dicha salvaguarda periódica a nivel de dicho servidor distante (60), y
- 15 dichas partes lógicas de datos persistentes existentes incluyendo cada una un elemento de datos de distinción;
- salvaguardar dicho elemento de datos de distinción en el almacenamiento de datos local (26) de cada parte lógica de datos persistentes existentes salvaguardados solamente a nivel del servidor distante (60); y
- 20 reconstruir los datos persistentes en el panel de control local (20) después de la reiniciación operativa del panel de control local (20),
- en donde, durante dicha etapa de reconstrucción, solamente dichas partes lógicas de datos persistentes existentes que tienen elementos de datos de distinción posteriores a dicho elemento de datos de distinción salvaguardados a nivel de dicho almacenamiento de datos local (26) son objeto de escritura desde dicho almacenamiento distante (70) y salvaguardados a nivel de dicho almacenamiento de datos local (26).
- 25
2. El método de almacenamiento de datos según la reivindicación 1, en donde dichos elementos de datos de distinción son marcas temporales.
- 30
3. El método de almacenamiento de datos según la reivindicación 1, en donde dicho almacenamiento de datos local (26) comprende una memoria no volátil.
- 35
4. El método de almacenamiento de datos según la reivindicación 3, en donde dicho almacenamiento de datos local (26) comprende una memoria instantánea.
- 40
5. El método de almacenamiento de datos según la reivindicación 1, en donde dicho almacenamiento de datos distante (70) comprende al menos un dispositivo entre dispositivos de memoria RAM y EEPROM.
- 45
6. El método de almacenamiento de datos según la reivindicación 5, en donde dicho almacenamiento de datos local (26) comprende una memoria instantánea.
- 50
7. Un sistema de seguridad (10) que comprende:
- 45 dispositivos de seguridad (40, 42) que generan datos persistentes;
- un sistema de control local (20) que recibe dichos datos persistentes desde dichos dispositivos de seguridad (40, 42), incluyendo dicho sistema de control local (10) un microprocesador (22) y una memoria no volátil (26);
- 50 un servidor (60) distante de dicho sistema de control local (20), incluyendo dicho servidor distante (60) un almacenamiento de datos distante (70) y estando en comunicación con dicho microprocesador del sistema de control local (22);
- 55 en donde dicho microprocesador del sistema de control local (22):
- transmite periódicamente partes lógicas de datos persistentes existentes al servidor distante (60) para salvaguardarlos en dicho almacenamiento de datos distante (70), comprendiendo dichas partes lógicas de datos persistentes existentes, cada una de ellas, un elemento de datos de distinción;
- 60 salvaguardar periódicamente dichas partes lógicas de datos persistentes existentes en dicha memoria no volátil (26) del sistema de control local menos frecuentemente que dichos datos persistentes son salvaguardados periódicamente en dicho almacenamiento de datos distante (70);
- 65 salvaguardar dicho elemento de datos de distinción en el almacenamiento de datos local (26) para cada parte lógica de datos persistentes existentes salvaguardados solamente a nivel del servidor distante (60), y

cuando se reinicia operativamente dicho sistema de control local (20), recupera desde dicho almacenamiento de datos distante (70) solamente dichas partes lógicas de datos persistentes existentes que tienen elementos de datos de distinción posteriormente a dicho elemento de datos de distinción salvaguardado en la memoria no volátil (26) del sistema de control de datos local.

- 5
- 8.** El sistema de seguridad según la reivindicación 7, en donde dichos elementos de datos de distinción son marcas temporales.
- 10 **9.** El sistema de seguridad según la reivindicación 7, en donde dicha memoria no volátil (26) comprende una memoria instantánea IC.
- 15 **10.** El sistema de seguridad según la reivindicación 9, en donde dicho almacenamiento de datos distante (70) comprende al menos un dispositivo de entre los dispositivos de memoria RAM y EEPROM.
- 11.** El sistema de seguridad según la reivindicación 7, en donde dicho almacenamiento de datos distantes (70) comprende al menos un dispositivo entre dispositivos de memoria RAM y EEPROM.

20

