



OFICINA ESPAÑOLA DE
PATENTES Y MARCAS

ESPAÑA

① Número de publicación: **2 288 340**

② Número de solicitud: 200500119

⑤ Int. Cl.:
G06F 21/06 (2006.01)
G11B 5/024 (2006.01)

⑫

PATENTE DE INVENCION

B1

⑫ Fecha de presentación: **21.01.2005**

⑬ Fecha de publicación de la solicitud: **01.01.2008**

Fecha de la concesión: **21.08.2008**

⑮ Fecha de anuncio de la concesión: **16.09.2008**

⑯ Fecha de publicación del folleto de la patente:
16.09.2008

⑰ Titular/es: **Universidade de Vigo**
Rúa Oporto, nº 1
36201 Pontevedra, ES

⑱ Inventor/es: **Méndez Reboredo, José Ramón;**
Rodríguez Martínez, Francisco Javier y
Fernández Riverola, Florentino

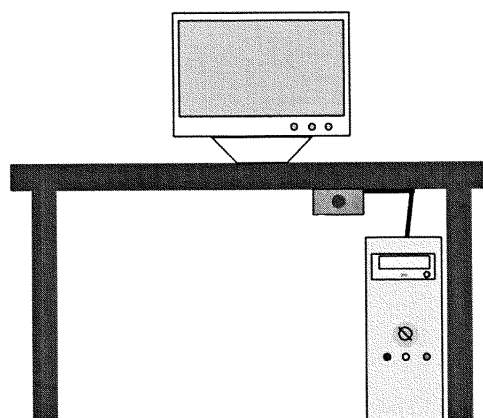
⑳ Agente: **No consta**

⑳ Título: **Dispositivo para la protección ante el espionaje industrial.**

㉑ Resumen:

Dispositivo para la protección ante el espionaje industrial. La presente invención hace referencia a un "Dispositivo para la protección ante el espionaje industrial" cuya finalidad es la de proteger a los usuarios finales de posibles actos de espionaje industrial en situaciones de riesgo de intento de robo de información en un sistema informático. Este dispositivo incluye una unidad controladora electrónica que permite activar, mediante un pulsador y/o distintos sensores cuyas señales de salida se procesan de forma inteligente, un circuito efector capaz de producir el borrado permanente de la información almacenada en cualquier dispositivo magnético, los cuales, por otra parte, son habituales en los equipos de procesamiento de información.

Se reivindica el dispositivo para la protección ante el espionaje industrial caracterizado porque permite el borrado físico de la información de medios de almacenamiento magnéticos de una forma sencilla para el usuario, compuesto por un circuito controlador que acciona un circuito efector mediante un elemento activador y basado en el uso de una unidad de desmagnetización que produce el borrado de medios magnéticos de almacenamiento de información generando un campo magnético de gran intensidad.



ES 2 288 340 B1

Aviso: Se puede realizar consulta prevista por el art. 37.3.8 LP.

DESCRIPCIÓN

Dispositivo para la protección ante el espionaje industrial.

La presente invención se refiere a un dispositivo cuya finalidad es la de proteger a un usuario de programas informáticos almacenados en un ordenador, de un posible espionaje industrial en situaciones de riesgo de robo de información. El mecanismo ha sido ideado para intentos de sustracción a mano armada o similar y permite, a través de un botón accesible o señales generadas por sensores (de presencia, de volumen, etc), la destrucción de forma rápida y eficaz de la información almacenada en sistemas informáticos.

Antecedentes

Hoy en día es muy habitual escuchar reflexiones sobre seguridad referidas a sistemas de información, informática, información y datos. Todos estos conceptos sobre seguridad, información e informática, están muy relacionados entre sí y con las actividades económicas que las empresas llevan a cabo. En este sentido, un sistema de información es un conjunto de elementos que interactúan entre sí con el fin de apoyar las actividades de una empresa o negocio, permitiendo el manejo de la información y el acceso rápido y fiable a datos concretos, utilizando para ello tecnologías basadas en la informática. Cada día, una empresa registra información sensible de diversa índole (de clientes, de proveedores, del proceso propio de transformación de las materias primas, contable, etc.), la cual permite que ésta pueda ejercer su actividad económica de forma satisfactoria. Es tal la necesidad de información, de su correcto acceso y mantenimiento eficaz, que su robo puede representar para las organizaciones la quiebra técnica.

La información se almacena habitualmente en dispositivos magnéticos u ópticos, aunque por su mayor velocidad de acceso, suelen utilizarse los primeros. Normalmente, las compañías disponen de centros seguros donde se guarda la información en medios de almacenamiento protegidos por complejos esquemas de copias de seguridad. El acceso a estos centros suele estar adecuadamente protegido en cuanto a medidas de seguridad y acceso se refiere, lo que implica que, generalmente, no será factible para un intruso acometer un robo de información.

Sin embargo, para el empleo de la información, ésta debe copiarse, por medio de una red de telecomunicaciones a un equipo donde finalmente se procesa por el usuario final. Debido a esta movilidad de información, los datos se guardan temporalmente y se permiten realizar operaciones sobre ellos. El almacenamiento temporal de los datos se produce en soportes magnéticos (habitualmente discos duros), que garantizan una velocidad considerable a la vez que permiten la reescritura.

Los sistemas de almacenamiento de información en medios magnéticos, utilizan la orientación selectiva de pequeñas partículas magnéticas depositadas en un sustrato mediante la acción de una cabeza lectora/grabadora. Esta cabeza está compuesta por una minúscula bobina que genera campos magnéticos cuando circula a través de ella una corriente eléctrica y permite magnetizar distintos sectores del medio de registro. Para escribir, las corrientes generadas están asociadas a la información que se quiere almacenar, de modo que la orientación de las partículas corresponde al registro de la información. Para leer, la cabeza

lectora/grabadora recorre la superficie del disco duro o de la cinta magnética realizando el proceso inverso y recuperando la información almacenada al detectar los campos magnéticos de las partículas.

El borrado de la información de medios magnéticos no se produce físicamente, sino que para conseguir una mayor rapidez, únicamente se borra una determinada entrada de una tabla de índices, por lo que si un soporte magnético de estas características es sustraído, se puede recuperar la información que almacena mediante el empleo de técnicas de análisis forense. En este sentido, si el medio de almacenamiento magnético ha sido soporte de información confidencial, es evidente que se compromete dicha condición.

En este sentido, la posibilidad de poder contar con un mecanismo que permita el borrado físico y real de los datos, conlleva una mejora a la hora de proteger la privacidad de la información manejada.

Descripción de la invención

El dispositivo objeto de esta invención presenta unas particularidades constructivas que permiten realizar un borrado físico de toda la información almacenada en medios magnéticos en un tiempo realmente pequeño. El dispositivo, situado dentro del ordenador, se activa mediante la pulsación de un botón conectado por medio de un hilo conductor a un mecanismo de borrado, el cual, lleva a cabo esta tarea actuando sobre el medio de almacenamiento magnético, mediante la generación de un intenso campo magnético.

De acuerdo con la invención, este dispositivo necesita ser alimentado eléctricamente con dos tensiones diferentes. La primera es de 220 voltios, con una intensidad de 25 o más amperios en corriente alterna que se puede obtener fácilmente de una red eléctrica doméstica. La segunda es de 5 voltios y 20 miliamperios en corriente continua, que se puede obtener directamente de las líneas de alimentación interna de los equipos de procesamiento de información actuales. Sin embargo, a pesar de que la alimentación puede ser obtenida del equipo de procesamiento de información y de la red eléctrica doméstica, resulta conveniente el uso de baterías o sistemas de alimentación ininterrumpida que garanticen la correcta alimentación incluso en el caso de que se produzca un fallo en el suministro eléctrico.

Con las líneas de alimentación eléctrica mencionadas, la unidad objeto de esta invención colocada de la forma que se relata más abajo, puede proceder al borrado físico de la información almacenada en medios de almacenamiento magnéticos evitando así, que ésta pueda ser recuperada mediante el uso de complejas técnicas de análisis.

Descripción de las figuras

Para completar la descripción que se está realizando y con objeto de facilitar la comprensión de las características de la invención, se acompaña a la presente memoria descriptiva un juego de dibujos en los que, con carácter ilustrativo y no limitativo, se ha representado lo siguiente:

La figura 1 muestra un ejemplo de realización del dispositivo objeto de la invención, especificando cada uno de los elementos que lo componen (controlador (11) y efector (12)).

La figura 2 muestra una posible disposición específica de los componentes del mecanismo, a fin de proteger la información corporativa de una mesa de atención al público en un puesto de información.

La figura 3 muestra la disposición del mecanismo

de borrado del medio magnético, parte fundamental de la presente invención.

Realización preferente de la invención

Como se puede observar en el ejemplo de realización mostrado en la figura 1, el dispositivo incluye dos partes autónomas: controlador (11) y efector (12). Cada una de estas unidades (controlador y efector) trabajan con corrientes eléctricas de distinta naturaleza (continua y alterna respectivamente) y, además, con distintas diferencias de potencial (5 y 220 voltios respectivamente). Por otro lado, cabe reseñar que la naturaleza del circuito controlador es digital, mientras que la del circuito efector es analógica. El controlador siempre permanece alimentado y en funcionamiento y se ocupa del control de la activación del circuito que alimenta al efector usando un elemento activador (13) que es capaz de cerrar un circuito de corriente alterna con diferencia de potencial de 220 voltios y una intensidad igual o superior a 25 amperios empleando, para ello, una corriente continua con una tensión de 5 voltios y una intensidad de 6 miliamperios. El flujo de electrones o corriente que actúa como señal del activador, para activar el efector, se produce a través de los cables (111) y (17) representados en la figura 1.

La alimentación del controlador se realiza a través de una fuente de alimentación conectada a los puntos (18) y (19) del circuito mientras que la del circuito efector se hará a través del punto (110) de la figura 1. El circuito controlador (11), ubicado en la caja 21 de la figura 2, se alimentará mediante dos cables de la interconexión lineal (23) representada en la figura 2.

Por otro lado, la interconexión lineal (23) soportará mediante un tercer cable, la señal de activación (17) del elemento activador (13), ambos en la figura 1.

En la caja (21) se ubica un conjunto de sensores (112) útiles para detectar una intrusión y que permiten un comportamiento inteligente de la presente invención, junto con un pulsador (211), que permite la activación manual del mecanismo. Obviamente el mecanismo debe disponer, al menos, de un sensor o un pulsador por el cual pueda ser activado.

Los sensores (112) pueden ser de diversa índole (de presencia, volumen, etc.) e incluso estar formados por sistemas complejos. Resulta aconsejable usar un sensor que permita, a través de un dispositivo de comunicación GSM, detectar si se ha recibido un mensaje SMS con un determinado formato, lo cual permitiría la destrucción de la información almacenada de forma remota, usando un teléfono móvil.

El dispositivo contiene un procesador de señales (16) que permite manejar, de forma inteligente, un conjunto de señales, de tal forma que, ante un inmi-

nente robo de información, activa una señal de salida en el cable (17) que permite la activación del circuito efector y, por tanto, el borrado del medio magnético.

Si se realiza una implementación con un pulsador (211) y/o sensores (112) simples de naturaleza digital, el circuito procesador de señales puede ser implementado fácilmente con sistemas digitales combinatoriales y secuenciales. En caso de que se usen sensores analógicos, con señales en serie o difíciles de interpretar, es necesario que el circuito controlador sea un pequeño procesador que disponga de conversores analógico-digitales y un software embebido capaz de procesar de forma inteligente las señales analógicas y digitales para producir la activación del mecanismo en el momento oportuno.

Como se puede observar en la figura 2, cada una de las partes autónomas (controlador y efector) se disponen en una ubicación diferente, situándose la primera en una pequeña caja (21) y la segunda dentro de la carcasa del ordenador personal (22).

Al producirse determinadas combinaciones de señales de los sensores y/o del pulsador (14), el circuito procesador de señales (16) generará una señal digital activa (estado alto) y permanente en el cable (17). Esta señal mantendrá activo el elemento activador (13) que cerrará el circuito efector (12). Este último circuito alimenta una unidad de desmagnetización (15), formada por una bobina y un núcleo de ferrita, que creará un campo magnético de una magnitud suficiente para eliminar de forma permanente la información almacenada en cualquier soporte magnético dentro del equipo de proceso de la información.

La unidad de desmagnetización (15) estará dotada de un electroimán (31) y, para el correcto funcionamiento de esta invención, deberá estar colocada con escasa separación del soporte de almacenamiento magnético (32) que se desea proteger. La figura 3 presenta una implementación posible de la unidad de desmagnetización. Adicionalmente, también se pueden colocar nuevas unidades de desmagnetización activadas por la señal de activación que portan los cables (17) y (111), para cada una de las cuales, habrá que emplear un nuevo elemento activador (13) y que se destinarán al borrado de otros medios de almacenamiento magnéticos.

Una vez descrita suficientemente la naturaleza de la invención, así como un ejemplo de realización preferente, se hace constar a los efectos oportunos que los materiales, forma, tamaño, disposición de los elementos descritos podrán ser modificados, siempre y cuando ello no suponga una alteración de las características esenciales de la invención que se reivindican a continuación.

REIVINDICACIONES

1. Dispositivo para la protección ante el espionaje industrial el cual está **caracterizado** por:

- a. El proceso de borrado se desencadena por medio de una serie de sensores (de presencia, volumen, etc.) (112) y/o un pulsador (19, 211) cuyas señales de salida se analizan de forma inteligente para detectar posibles intrusiones.
- b. Dispone de un circuito controlador (11) y un circuito efector (12). El primero permite el borrado del dispositivo magnético (32), mientras que el segundo permite determinar de forma inteligente el instante en el que se produce la intrusión.
- c. Su funcionamiento está basado en una unidad de desmagnetización (15) que permite el borrado físico del medio magnético, generando un campo magnético de gran intensidad.

2. Dispositivo para la protección ante el espionaje industrial según reivindicación 1, **caracterizado** porque su activación se puede hacer a través de un pulsador (14) o sensores de diversa índole (112) ubicados

en un circuito controlador (11) que opera con corriente continua de una intensidad baja. Dicha activación se produce de forma inteligente cuando se detecta una intrusión. El dispositivo dispone de un circuito procesador de señales (16) que permite detectar intrusiones a través de los datos obtenidos de los sensores (112) y del pulsador (14).

3. Dispositivo para la protección ante el espionaje industrial según reivindicación 1, **caracterizado** por estar conformado por un circuito controlador (11) capaz de activar circuito efector (12) mediante un elemento activador (13). La activación se llevará a cabo mediante una señal eléctrica digital que el circuito controlador transmite al elemento activador (13) en el instante en el que detecta una posible intrusión. El elemento activador (13) tiene la capacidad de activar el circuito efector (12), desencadenando del borrado el medio magnético protegido.

4. Dispositivo para la protección ante el espionaje industrial según reivindicación 1, **caracterizado** por disponer de una unidad de desmagnetización (15) cuyo fundamento se basa en la acción de un electroimán (31) capaz de generar un campo magnético suficientemente intenso como para permitir la desorientación de las partículas magnéticas que se emplazan en un soporte magnético. El borrado logrado mediante este dispositivo resulta permanente e irreversible.

30

35

40

45

50

55

60

65

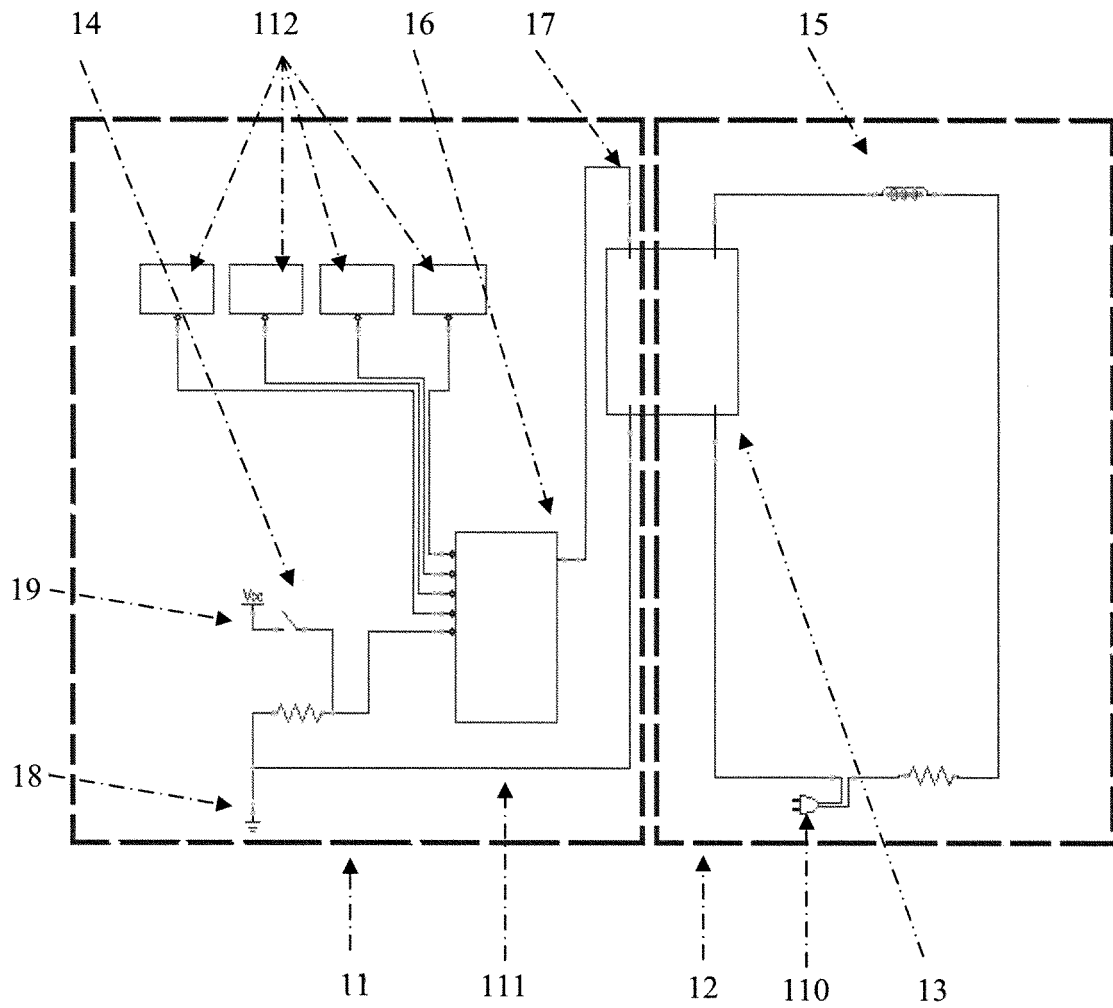


Fig. 1

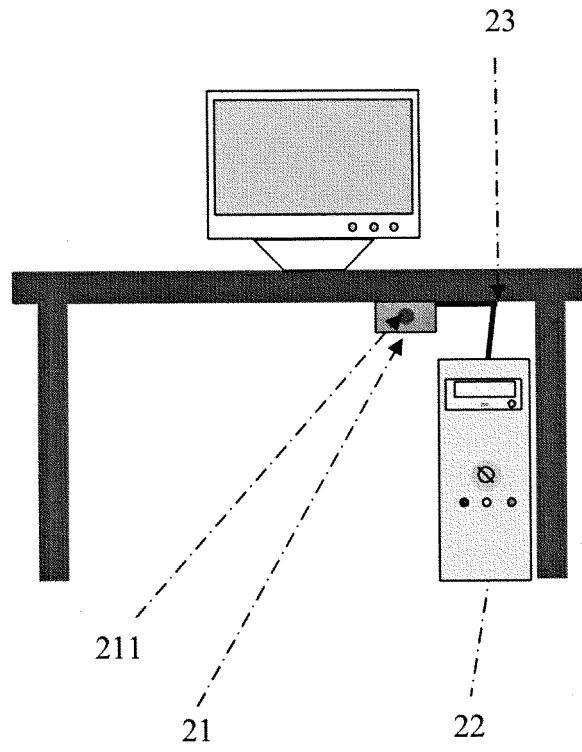


Fig. 2

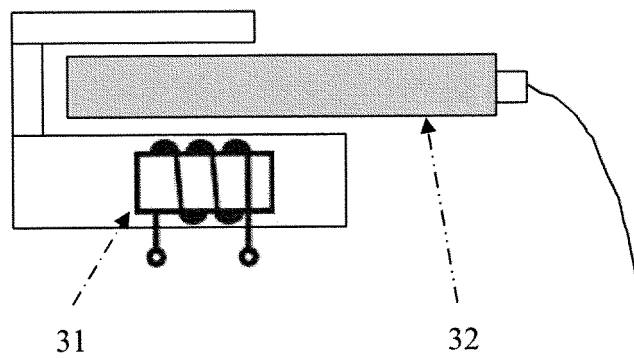


Fig. 3



OFICINA ESPAÑOLA DE
PATENTES Y MARCAS

ESPAÑA

① ES 2 288 340

② Nº de solicitud: 200500119

③ Fecha de presentación de la solicitud: **21.01.2005**

④ Fecha de prioridad:

INFORME SOBRE EL ESTADO DE LA TÉCNICA

⑤ Int. Cl.: **G06F 21/06** (2006.01)
G11B 5/024 (2006.01)

DOCUMENTOS RELEVANTES

Categoría	Documentos citados	Reivindicaciones afectadas
Y	US 2005192453 A1 (ECKL et al.) 01.09.2005, resumen; párrafos [1-4],[13-17].	1-4
Y	FR 2723609 A1 (ESCAL PHILIPPE) 16.02.1996, resumen; página 2, línea 24 - página 3, línea 12; página 3, línea 27 - página 4, línea 32; figura 1.	1,4
A	WO 9703397 A1 (BENKTA CONSULTING AB) 30.01.1997, resumen; página 1, línea 34 - página 2, línea 36; página 3, línea 6 - página 7, línea 22; figura 1.	1,2

Categoría de los documentos citados

X: de particular relevancia

Y: de particular relevancia combinado con otro/s de la misma categoría

A: refleja el estado de la técnica

O: referido a divulgación no escrita

P: publicado entre la fecha de prioridad y la de presentación de la solicitud

E: documento anterior, pero publicado después de la fecha de presentación de la solicitud

El presente informe ha sido realizado

para todas las reivindicaciones

para las reivindicaciones nº:

Fecha de realización del informe 10.12.2007	Examinador A. Figuera González	Página 1/1
---	--	---------------