(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 768 281**

(51) Int. CI.:

H04L 9/00 (2006.01)
H04L 29/06 (2006.01)
G06F 21/10 (2013.01)
G06F 21/60 (2013.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **20.12.2013 PCT/US2013/076810**

(87) Fecha y número de publicación internacional: **03.07.2014 WO14105673**

(96) Fecha de presentación y número de la solicitud europea: **20.12.2013 E 13866968 (4)**

(97) Fecha y número de publicación de la concesión europea: **23.10.2019 EP 2939361**

(54) Título: **Sistemas y métodos para reducción de riesgo de red**

(30) Prioridad:

28.12.2012 US 201261746813 P
15.03.2013 US 201313835611

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
22.06.2020

(73) Titular/es:

EQUIFAX, INC. (100.0%)
1550 Peachtree Street, N. W.
Atlanta, GA 30309, US

(72) Inventor/es:

MAGILL, ADAM;
SMITH, BENJAMIN;
NEDOSTUP, NICHOLAS y
SPINELLI, ANTHONY

(74) Agente/Representante:

ELZABURU, S.L.P

DESCRIPCIÓN

Sistemas y métodos para reducción de riesgo de red

Referencia cruzada a solicitudes relacionadas

Esta solicitud reivindica la prioridad de la Solicitud de Patente de EE. UU. No. 13/835,611 presentada el 15 de marzo de 2013, y reivindica el beneficio de la Solicitud Provisional de EE. UU. No. 61/746,813, presentada el 28 de diciembre de 2012.

Campo técnico

La presente divulgación generalmente se refiere a sistemas y métodos implementados por ordenador para reducir los riesgos asociados con la comunicación de red para una organización.

Antecedentes

Las redes pueden implicar el intercambio electrónico de contenido. Los sistemas y métodos son deseables y pueden analizar datos para reducir los riesgos para una organización en relación con el intercambio electrónico de contenido con fuentes externas a la organización. El documento US2012102545 divulga un método para calcular un puntaje de reputación para un dominio (por ejemplo, representado por una URL), donde la calificación de reputación indica si dicho dominio es malicioso o seguro.

Resumen

En un aspecto, la información variable se extrae de los datos del registro de actividad de la red en un dispositivo de procesamiento. Los datos del registro de actividad de la red incluyen una solicitud de acceso al contenido de un usuario en una organización para una fuente de contenido de la red. La información variable incluye un número de veces que se ha solicitado el contenido de la fuente de contenido de la red, un volumen de usuarios de organización que han solicitado el contenido de la fuente de contenido de red y un período de tiempo para cuyo tráfico con respecto a la red se ha detectado. La información variable se puntúa para generar una calificación de riesgo que indica para la organización un riesgo relativo asociado con la fuente de contenido de la red. Se determina un nivel de control de acceso para la fuente de contenido de la red en función de la calificación de riesgo y una política de acceso al contenido para la organización. El acceso del usuario en la organización a la fuente de contenido de la red se controla según el nivel de control de acceso.

En otro aspecto, un sistema incluye un dispositivo servidor. El dispositivo servidor incluye un procesador y un medio de almacenamiento legible por ordenador no transitorio que contiene instrucciones que, cuando se ejecutan en el procesador, hacen que el procesador realice operaciones. Las operaciones incluyen:

extraer información variable de los datos del registro de actividad de la red que incluye una solicitud de acceso al contenido de un usuario en una organización para una fuente de contenido de la red, la información variable incluye un número de veces que se ha solicitado el contenido de la fuente de contenido de red, un volumen de usuarios de organización que han solicitado un contenido de la fuente de contenido de la red, y un período de tiempo durante el cual se ha detectado tráfico con respecto a la fuente de contenido de la red;

calificar la información variable para generar una calificación de riesgo que indica para la organización un riesgo relativo asociado con la fuente de contenido de la red;

determinar un nivel de control de acceso para la fuente de contenido de la red en función de la calificación de riesgo y una política de acceso al contenido para la organización; y

controlar el acceso del usuario en la organización a la fuente de contenido de la red de acuerdo con el nivel de control de acceso.

En otro aspecto, se proporciona un producto de programa informático incorporado de forma tangible en un medio de almacenamiento legible por máquina no transitorio que incluye instrucciones configuradas para hacer que un aparato de procesamiento de datos:

extraiga información variable de datos de registro de actividad de red que incluye una solicitud de acceso de contenido de un usuario en una organización para una fuente de contenido de la red, la información variable incluye un número de veces que se ha solicitado el contenido de la fuente de contenido de la red, un volumen de usuarios de la organización que han solicitado una fuente de contenido de la red, y un período de tiempo durante el cual se ha detectado tráfico con respecto a la fuente de contenido de la red;

califique la información variable para generar una calificación de riesgo que indica para la organización un riesgo relativo asociado con la fuente de contenido de la red;

determine un nivel de control de acceso para la fuente de contenido de la red en función de la calificación de riesgo y una política de acceso al contenido para la organización; y

controle el acceso del usuario en la organización a la fuente de contenido de la red de acuerdo con el nivel de control de acceso.

La invención se divulga en las reivindicaciones adjuntas. Los detalles de uno o más aspectos y ejemplos se exponen en los dibujos adjuntos y la descripción a continuación. Otras características y aspectos se harán evidentes a partir de la descripción, los dibujos y las reivindicaciones.

Breve descripción de los dibujos

La figura 1 representa un ejemplo de un entorno que incluye un sistema de análisis de datos.

La figura 2 representa un ejemplo de un sistema de análisis de datos que incluye múltiples servidores.

La figura 3 es un diagrama de bloques de un ejemplo de un servidor analítico.

La figura 4 es un diagrama de flujo de datos de procesamiento de datos de ejemplo en relación con una solicitud de usuario de la organización para contenido de una fuente de contenido de red.

La figura 5 es un diagrama de flujo de datos de un ejemplo de un proceso para extraer información variable de datos de registro de actividad.

La figura 6 es una pirámide de riesgo que representa un ejemplo de un continuo de seguridad que puede estar asociado con una fuente de contenido de red fuera de la red de una organización.

Descripción detallada

Ciertos aspectos incluyen sistemas y métodos para reducir los riesgos asociados con el uso de la red, tales como acceder al contenido desde direcciones de dominio de Internet y/o correo electrónico. Los riesgos pueden incluir contenido ejecutable incluido en una página web o correo electrónico que puede enviar malware, spyware u otra programación no deseada a un dispositivo dentro de la red de una organización. La reducción del riesgo de los hábitos de navegación y correo electrónico de los usuarios, por ejemplo, se puede lograr al menos en parte analizando los hábitos de navegación y correo electrónico de los usuarios de una organización (por ejemplo, empleados) a través de registros de tráfico. Se puede obtener una calificación de seguridad o riesgo de un dominio de Internet/remitente de correo electrónico evaluando ciertos factores determinados a partir de los registros de tráfico. Dichos factores pueden incluir (A) el número de veces que los usuarios dentro de la organización hicieron solicitudes al dominio/remitente, (B) el volumen de usuarios dentro de la organización que realiza una solicitud al dominio/remitente, y (C) el período de tiempo en que se han realizado solicitudes de los usuarios dentro de la organización al dominio/remitente.

Mediante el análisis estadístico de los factores, se puede derivar una calificación relativa para un dominio de Internet (o un remitente o destinatario de correo electrónico, según sea el caso). La calificación se puede aprovechar junto con los puntos de cumplimiento de políticas existentes, como los servidores proxy, para tomar una acción definida. La acción puede incluir permitir el acceso al dominio/remitente, pero limitar el contenido que los usuarios dentro de la organización pueden recibir del dominio/remitente hasta que aumente la calificación asociada con el dominio/remitente. Por ejemplo, los usuarios dentro de una organización pueden ser incentivados para acceder a un dominio a pesar de que el contenido accesible desde ese dominio podría estar limitado para que el dominio sea considerado “seguro” de modo que sea innecesario intentar eludir la seguridad del usuario. En algunos aspectos, se puede calcular una calificación para un dominio y la acción se puede aplicar sustancialmente en tiempo real con respecto a una solicitud de un usuario dentro de la organización para ese dominio.

Un dominio puede percibirse como arriesgado al principio, pero luego puede considerarse “seguro” por, por ejemplo, más usuarios dentro de una organización que acceden al dominio con el tiempo. Por ejemplo, el sistema puede determinar con el tiempo con un grado relativamente alto de seguridad de que un dominio es de mayor riesgo (por ejemplo, no se accede con frecuencia, solo acceden unos pocos usuarios dentro de la organización y solo durante un corto período de tiempo) o de menor riesgo (por ejemplo, a menudo acceden muchos usuarios dentro de la organización durante un período de tiempo más largo). Las defensas a los riesgos pueden ser impulsadas en parte por la dinámica de grupo de los usuarios dentro de una organización. Los sistemas de acuerdo con algunos aspectos pueden evaluar el riesgo de acuerdo con una cantidad de usuarios dentro de la organización sin ser necesariamente tan intrusivos como usar informes con el contenido exacto al que accede el usuario.

Al aprovechar el análisis a través de un sistema automatizado, una organización puede restringir dinámicamente el contenido activo de un dominio o remitente de correo electrónico, reduciendo así la exposición al riesgo de la organización. El análisis y la calificación de dominios y correos electrónicos pueden ser diferentes para diferentes organizaciones, dependiendo de lo que se “conoce” dentro de una organización y las políticas deseadas para una organización. Por ejemplo, los dominios a los que acceden con frecuencia los usuarios dentro de la organización A no pueden ser accedidos, por lo general, los usuarios dentro de la organización B, como esos mismos dominios pueden

tener una calificación más baja para la organización B. Además, una organización puede requerir que se acceda a dominios por un período de tiempo más largo que otra organización antes de que dichos dominios se consideren “seguros”.

La figura 1 es un ejemplo de un entorno en el que ciertos aspectos pueden implementarse utilizando un sistema 102 de análisis de datos. El sistema 102 de análisis de datos puede ser para una organización y puede comunicarse a través de comunicación por cable o inalámbrica con dispositivos de la organización utilizados por los usuarios dentro de la organización. Los dispositivos de organización como se muestra en la figura 1 incluye un ordenador 104, un ordenador 106 portátil, un dispositivo 108 informático móvil y un ordenador 110 tipo tableta. Se pueden usar otros tipos de dispositivos. El sistema 102 de análisis de datos puede comunicarse a través de una red 112 con fuentes de contenido de red, tales como dispositivos 114a-n de servidor web y dispositivos 116a-n de correo electrónico, que son externos a la organización. Los dispositivos 114a-n de servidor web pueden proporcionar páginas web que incluyen contenido en respuesta a las solicitudes de los usuarios de los dispositivos de la organización. Los dispositivos 116a-n de correo electrónico pueden proporcionar correos electrónicos que incluyen contenido a los usuarios de los dispositivos de la organización. El sistema 102 de análisis de datos puede analizar el tráfico entre los dispositivos de la organización y los dispositivos del servidor 114a-n web y los dispositivos 116a-n de correo electrónico, y puede configurarse para realizar acciones tales como limitar el contenido que se entrega a los dispositivos de la organización dentro de la organización.

El sistema 102 de análisis de datos puede incluir un dispositivo o múltiples dispositivos que analizan juntos los datos de actividad de la red y controlan el acceso a las fuentes de contenido de la red en función de los riesgos relativos. La figura 2 representa un ejemplo del sistema 102 de análisis de datos que incluye múltiples servidores. Los servidores incluyen un servidor 202 de contenido, un servidor 204 de registro, un servidor 206 analítico y un servidor 208 de cumplimiento. El servidor 202 de contenido puede recibir solicitudes de los usuarios de la organización para contenido de fuentes de contenido de red. El servidor 204 de registro puede determinar información variable a partir de datos de registro, incluidas las solicitudes de contenido, recibidas del servidor 202 de contenido. El servidor 206 analítico puede generar calificaciones de riesgo a partir de la información variable. El servidor 208 de aplicación puede determinar los niveles de control de acceso para las fuentes de contenido de la red en función de las calificaciones de riesgo.

La figura 3 representa un diagrama de bloques con un ejemplo del servidor 206 analítico. Se pueden utilizar otras implementaciones, tales como implementaciones que incluyen múltiples dispositivos, cada uno configurado para realizar funciones seleccionadas.

El servidor 206 analítico incluye un procesador 302 que puede ejecutar código almacenado en un medio tangible legible por ordenador en una memoria 304, para hacer que el servidor 206 analítico realice funciones. El servidor 206 analítico puede incluir cualquier dispositivo que pueda procesar datos y ejecutar código que es un conjunto de instrucciones para realizar funciones. Los ejemplos de los dispositivos incluyen un servidor de base de datos, un servidor web, un ordenador personal de escritorio, un ordenador personal portátil, un dispositivo de servidor, un dispositivo informático portátil y un dispositivo móvil.

Los ejemplos del procesador 302 incluyen un microprocesador, un circuito integrado de aplicación específica (ASIC), una máquina de estado u otro procesador adecuado. El procesador 302 puede incluir un procesador o cualquier número de procesadores. El procesador 302 puede acceder al código almacenado en la memoria 304 a través de un bus. La memoria 304 puede ser cualquier medio legible por ordenador no transitorio configurado para incorporar código tangiblemente y puede incluir dispositivos electrónicos, magnéticos u ópticos. Los ejemplos de la memoria 304 incluyen memoria de acceso aleatorio (RAM), memoria de solo lectura (ROM), un disquete, disco compacto, dispositivo de video digital, disco magnético, un ASIC, un procesador configurado u otro dispositivo de almacenamiento.

Las instrucciones pueden almacenarse en la memoria 304 como código ejecutable. Las instrucciones pueden incluir instrucciones específicas del procesador generadas por un compilador y/o un intérprete a partir del código escrito en cualquier lenguaje de programación de ordenadores adecuado. Las instrucciones pueden incluir una o más aplicaciones, tales como un motor 306 analítico, que, cuando es ejecutado por el procesador 302, puede hacer que el servidor 206 analítico realice funciones. El motor 306 analítico puede ejecutarse para calificar información variable (es decir, factores) de acuerdo con la política de seguridad de una organización. También se incluye en la memoria 304 un almacén 308 de datos que puede almacenar información recibida por el servidor 206 analítico e información derivada por el servidor 206 analítico.

Cada uno de los servidores 202 de contenido, el servidor 204 de registro y el servidor 208 de cumplimiento puede ser similar al servidor 206 analítico de la figura 3. El servidor 202 de contenido puede incluir un motor de solicitud de contenido que genera registros que incluyen solicitudes de contenido e información asociada. El servidor 204 de registro puede incluir un motor de inteligencia que puede derivar información variable de los registros. El servidor 208 de cumplimiento puede incluir un motor de acción que puede limitar el acceso al contenido desde una fuente de contenido de red en función de una calificación de riesgo.

La figura 4 es un diagrama de flujo de datos que incluye un ejemplo de procesos del sistema 102 de análisis de datos en relación con la solicitud de un usuario de la organización para contenido de una fuente de contenido de red. El diagrama de flujo de datos se describe con referencia a las figuras 1-3, pero se pueden usar otras implementaciones.

Una solicitud 402 de acceso al contenido de un dispositivo de la organización controlada por un usuario de la organización puede ser recibida por el servidor 202 de contenido en el sistema 102 de análisis de datos. La solicitud 402 de acceso al contenido puede ser una solicitud de contenido de un dispositivo de servidor web o correo electrónico desde un dispositivo de correo electrónico y puede incluir el nombre de usuario del usuario de la organización que realiza la solicitud.

El servidor 202 de contenido realiza un proceso 404 de formación de datos de registro de actividad utilizando la solicitud de acceso al contenido. Los datos 406 de registro de actividad pueden incluir actividad de red para usuarios dentro de la organización. La actividad de red puede incluir solicitudes de contenido web y/o solicitudes para recibir correos electrónicos de fuentes externas a la organización. En algunos aspectos, el servidor 202 de contenido genera los datos 406 de registro de actividad como datos de registro de actividad de proxy de archivo plano.

El servidor 204 de registro realiza un proceso 408 de extracción de información variable de los datos del registro de actividad. La información 410 variable puede incluir el número de veces que se ha solicitado contenido de la fuente de contenido de red, el volumen de usuarios de la organización que han solicitado un contenido de la fuente de contenido de red y un período de tiempo durante el cual el tráfico con respecto a la fuente de contenido de red ha sido detectado.

La figura 5 representa un diagrama de flujo de datos de un ejemplo de un proceso para extraer información variable de datos de registro de actividad. Los datos de registro de actividad pueden incluir datos 502 de registro de actividad actual y datos 504 de registro de actividad histórica. Los datos 502 de registro de actividad actual pueden ser actividades de red sustancialmente contemporáneas para procesar, o de lo contrario la solicitud más actual de contenido de la fuente de contenido de red. Los datos 504 de registro de actividad histórica pueden ser actividad de red que ha ocurrido previamente durante una cantidad de tiempo preestablecida antes de la solicitud más actual de contenido de la fuente de contenido de red.

El servidor 204 de registro realiza un proceso 506 de clasificación de los datos del registro de actividad. Por ejemplo, el servidor 204 de registro puede ejecutar un proceso de filtrado en los datos de registro de actividad para identificar los datos de registro de actividad asociados con la misma fuente de contenido de red que la fuente de contenido de red desde la cual se solicita actualmente el contenido. La salida del proceso de clasificación puede ser atributos de datos sobre la fuente de contenido de la red, como el nombre de dominio y la dirección del Protocolo de Internet (“IP”) de la fuente de contenido de la red 508 (o la identificación del remitente o destinatario del correo electrónico, según sea el caso), los nombres de usuario de los usuarios de la organización que tienen o solicitan contenido de la fuente 510 de contenido de red, y las horas y fechas de las solicitudes 512.

El servidor 204 de registro realiza un proceso 514 para determinar información variable a partir de los atributos de datos. La información variable puede incluir la cantidad de veces que se solicita contenido de la fuente de contenido de la red, como el dominio web o el remitente 516 de correo electrónico, el volumen de usuarios que solicitan contenido de la fuente 518 de contenido de red, y el período de tiempo durante el cual el tráfico de red es detectado para la fuente 520 de contenido de red. Otros tipos de información variable, como si se accedió a un dominio utilizando el nombre de dominio o una dirección IP insertada en un navegador web, pueden alternativamente o también derivarse. El servidor 204 de registro puede derivar la información variable de los atributos de datos, por ejemplo, aplicando lógica difusa u otro proceso analítico de datos a los atributos de datos.

Volviendo a la figura 4, el servidor 206 analítico realiza un proceso 412 de calificación de la información variable para generar una calificación 414 de riesgo. En algunos aspectos, la calificación 414 de riesgo se determina multiplicando cada tipo de información variable por una ponderación preseleccionada y luego multiplicando cada tipo de información variable ponderada. El motor 306 analítico del servidor 206 analítico puede calificar la información variable de acuerdo con una política de seguridad de una organización que puede especificar, por ejemplo, el peso relativo que debería aplicarse a cada tipo de información variable. La calificación se puede usar para evaluar la seguridad relativa del dominio, el remitente del correo electrónico u otro tipo de fuente de contenido de la red.

El servidor 208 de cumplimiento realiza un proceso 418 para determinar un nivel de acceso al contenido para la fuente de contenido de la red basado en la calificación 414 de riesgo y una política 416 de acceso al contenido de la organización. El nivel de acceso al contenido puede incluir permitir el acceso total al contenido de la fuente de contenido de la red, permitir el acceso a parte del contenido de la red, pero no todo, o impedir el acceso al contenido de la fuente de contenido de la red. La política 416 de acceso al contenido puede especificar un umbral de riesgo de la organización. En algunos aspectos, el nivel de acceso al contenido se determina comparando la calificación 414 de riesgo con el umbral de riesgo en la política 416 de acceso al contenido de la organización. El servidor 208 de cumplimiento puede generar un comando 420 de control de acceso al contenido que puede implementar el nivel de acceso al contenido para la fuente de contenido de la red, tal como limitando el contenido que el usuario de la organización puede recibir de la fuente de contenido de la red.

En algunos aspectos, muchos usuarios que realizan solicitudes a una fuente de contenido de red en el transcurso de un período de tiempo significativo pueden dar como resultado que el sistema 102 de análisis de datos determine que la fuente de contenido de red es una fuente de contenido segura de modo que el acceso completo al contenido desde la fuente de contenido de red está permitido para los usuarios dentro de la organización. Una fuente de contenido de red puede clasificarse inicialmente como insegura de tal manera que el sistema 102 de análisis de datos limita el

contenido que un usuario de la organización puede recibir de la fuente de contenido de red. En un momento posterior, la calificación para la fuente de contenido de la red puede cambiar en función de los valores de uno o más de los tipos de variables y hacer que la clasificación de la fuente de contenido de la red cambie a “segura”, de modo que el sistema 102 de análisis de datos permite que se reciba todo o la mayoría del contenido de la fuente de contenido de la red.

La figura 6 es una pirámide de riesgo que representa un ejemplo de un continuo de seguridad que puede estar asociado con una fuente de contenido de red fuera de la red de una organización. A medida que aumenta el número de usuarios que solicitan la fuente de contenido de la red, aumenta el volumen de usuarios que solicitan la fuente de contenido de la red, y aumenta la cantidad de tiempo, como la cantidad de días, durante los cuales se accede a la fuente de contenido de la red, la fuente de contenido de la red puede clasificarse de mayor riesgo a menor riesgo y luego a una clasificación segura. El sistema 102 de análisis de datos puede limitar la recepción de contenido desde la fuente de contenido de la red a un nivel que depende del nivel de riesgo asociado con la fuente de contenido de la red. Por ejemplo, si la fuente de contenido de la red se clasifica como altamente riesgosa (por ejemplo, en la parte inferior del continuo), se puede evitar que se reciba más contenido y más tipos de contenido de la fuente de contenido de la red en comparación con una fuente de contenido de la red que está clasificado como menos arriesgado, pero aún no como fuente segura de contenido de red.

Cada uno de los tipos de variables puede tener una pendiente diferente a las pendientes lineales representadas en la pirámide. La pendiente, por ejemplo, puede representar la ponderación que se puede aplicar a los factores basados en la política de acceso de una organización, que puede asociar más peso a un tipo de variable que a otros tipos de variables. Por ejemplo, un tipo de variable asociada con un peso bajo puede tener una pendiente más pronunciada, de modo que se necesitan aumentos menos extensos para ese tipo de variable para que una fuente de contenido de la red esté más cerca de ser clasificada como una fuente de contenido de red segura. La ponderación puede equipararse a la tolerancia relativa al riesgo, organización por organización.

En algunos aspectos, se necesita un aumento en los tres tipos de variables para que una fuente de contenido de red se acerque más a ser clasificada como una fuente de contenido de red segura. Por ejemplo, un aumento en la cantidad de veces que se solicita una fuente de contenido de red y en el volumen de usuarios que solicitan la fuente de contenido de red sin un aumento en el período de tiempo para tales solicitudes puede no mejorar la calificación de riesgo relativo para la fuente de contenido de red. Además, una fuente de contenido de red también puede volverse más riesgosa con el tiempo si, por ejemplo, los niveles en uno o más de los tipos de variables disminuyen.

Ciertos aspectos del tema y las operaciones funcionales descritas en esta especificación pueden implementarse en circuitos electrónicos digitales, o en software, firmware o hardware de ordenador, incluyendo las estructuras divulgadas en esta especificación y sus equivalentes estructurales, o en combinaciones de uno o más de ellos. Ciertos aspectos del tema descrito en esta especificación pueden implementarse como uno o más productos de programas de ordenador, es decir, uno o más módulos de instrucciones de programas de ordenador codificados en un medio legible por ordenador para ejecución o para controlar la operación del aparato de procesamiento de datos.

El medio legible por ordenador puede ser un dispositivo de almacenamiento legible por máquina, un sustrato de almacenamiento legible por máquina, un dispositivo de memoria, una composición de materia que efectúa una comunicación propagada legible por máquina, o una combinación de uno o más de ellos. El término “dispositivo de procesamiento de datos” abarca todos los aparatos, dispositivos y máquinas para procesar datos, incluyendo a modo de ejemplo un procesador programable, un ordenador o múltiples procesadores u ordenadores. El dispositivo puede incluir, además del hardware, código que crea un entorno de ejecución para el programa informático en cuestión, por ejemplo, código que constituye el firmware del procesador, una pila de protocolos, un sistema de gestión de bases de datos, un sistema operativo o una combinación de uno o más de ellos.

Un programa de ordenador (también conocido como programa, software, aplicación de software, secuencia de comandos o código), puede escribirse en cualquier forma de lenguaje de programación, incluyendo lenguajes compilados o interpretados, y puede implementarse en cualquier forma, incluyendo como un programa independiente o como un módulo, componente, subrutina u otra unidad adecuada para su uso en un entorno informático. Un programa de ordenador no necesariamente corresponde a un archivo en un sistema de archivos. Un programa puede almacenarse en una parte de un archivo que contiene otros programas o datos (por ejemplo, en una o más secuencias de comandos almacenadas en un documento de lenguaje de marcado), en un solo archivo dedicado al programa en cuestión o en múltiples archivos coordinados (por ejemplo, archivos que almacenan uno o más módulos, subprogramas o partes de código). Un programa de ordenador puede implementarse para ejecutarse en un ordenador o en varios ordenadores que se encuentran en un sitio o distribuidas en varios sitios e interconectados por una red de comunicación.

Los procesos y flujos lógicos descritos en esta especificación pueden ser realizados por uno o más procesadores programables que ejecutan uno o más programas de ordenador para realizar funciones operando datos de entrada y generando salida. Los procesos y los flujos lógicos también pueden ser realizados por, y un dispositivo también puede implementarse como un circuito lógico de propósito especial, por ejemplo, un FPGA (matriz de compuerta programable en campo) o un ASIC.

Los procesadores adecuados para la ejecución de un programa informático incluyen, a modo de ejemplo, microprocesadores de uso general y especial, y uno o más procesadores de cualquier tipo de ordenador digital. Generalmente, un procesador recibirá instrucciones y datos de una memoria de solo lectura o una memoria de acceso aleatorio o ambas. Los elementos esenciales de un ordenador son un procesador para realizar instrucciones y uno o más dispositivos de memoria para almacenar instrucciones y datos. En general, un ordenador también incluirá, o estará operativamente acoplada para recibir datos o transferir datos a, o ambos, uno o más dispositivos de almacenamiento masivo para almacenar datos, por ejemplo, discos magnéticos, magnetoópticos o discos ópticos. Sin embargo, un ordenador no necesita tener tales dispositivos. Además, un ordenador puede integrarse en otro dispositivo, por ejemplo, un teléfono móvil, un asistente digital personal (PDA), un reproductor de audio móvil, un receptor del Sistema de Posicionamiento Global (GPS), por nombrar solo algunos. Los medios legibles por ordenador adecuados para almacenar instrucciones y datos de programas de ordenador incluyen todas las formas de memoria no volátil, medios y dispositivos de memoria, incluidos, por ejemplo, dispositivos de memoria semiconductores, por ejemplo, EPROM, EEPROM y dispositivos de memoria flash; discos magnéticos, por ejemplo, discos duros internos o discos extraíbles; discos magnetoópticos; y discos CD ROM y DVD ROM. El procesador y la memoria pueden complementarse o incorporarse en un circuito lógico de propósito especial.

Para proporcionar interacción con un usuario, ciertos aspectos del tema descrito en esta especificación se pueden implementar en un ordenador que tiene un dispositivo de visualización, por ejemplo, un monitor CRT (tubo de rayos catódicos) a LCD (pantalla de cristal líquido), para mostrar información al usuario y un teclado y un dispositivo señalador, por ejemplo, un mouse o una bola de seguimiento, mediante los cuales el usuario puede proporcionar información al ordenador. También se pueden usar otros tipos de dispositivos para proporcionar interacción con un usuario; por ejemplo, la retroalimentación proporcionada al usuario puede ser cualquier forma de retroalimentación sensorial, por ejemplo, retroalimentación visual, retroalimentación auditiva o retroalimentación táctil; y la entrada del usuario se puede recibir en cualquier forma, incluida la entrada acústica, de voz o táctil.

Ciertos aspectos del tema descrito en esta especificación pueden implementarse en un sistema informático que incluye un módulo de servicio, por ejemplo, como un servidor de datos, o que incluye un componente de middleware, por ejemplo, un servidor de aplicaciones, o que incluye un componente de módulo de interfaz, por ejemplo, un ordenador cliente que tiene una interfaz gráfica de usuario o un navegador web a través del cual un usuario puede interactuar con una implementación del tema descrito en esta especificación, o cualquier combinación de uno o más módulos de servicio, middleware, o módulos de interfaz. Los componentes del sistema pueden estar interconectados por cualquier forma o medio de comunicación de datos digitales, por ejemplo, una red de comunicación. Los ejemplos de redes de comunicación incluyen una red de área local (“LAN”) y una red de área amplia (“WAN”), por ejemplo, Internet.

El sistema informático puede incluir clientes y servidores. Un cliente y un servidor generalmente están alejados entre sí y generalmente interactúan a través de una red de comunicación. La relación de cliente y servidor surge en virtud de los programas informáticos que se ejecutan en los ordenadores respectivos y que tienen una relación de servidor cliente entre sí.

Si bien esta especificación contiene muchos detalles, estos no deben interpretarse como limitaciones en el alcance o de lo que se puede reclamar en una solicitud o patente que reivindica la prioridad aquí o de otro modo, sino más bien como descripciones de características específicas de aspectos particulares. Ciertas características que se describen en esta especificación en el contexto o aspectos separados también se pueden implementar en combinación en una sola implementación. Por el contrario, varias características que se describen en el contexto de un solo aspecto también se pueden implementar en múltiples aspectos por separado o en cualquier subcombinación adecuada. Además, aunque las características pueden describirse anteriormente como que actúan en ciertas combinaciones e incluso reivindicarse inicialmente como tales, una o más características de una combinación reivindicada pueden en algunos casos eliminarse de la combinación, y la combinación reivindicada puede dirigirse a una subcombinación o variación de una subcombinación

De manera similar, aunque las operaciones se representan en los dibujos en un orden particular, esto no debe entenderse como que requiere que tales operaciones se realicen en el orden particular mostrado o en orden secuencial, o que todas las operaciones ilustradas se realicen para lograr resultados. En ciertas circunstancias, la multitarea y el procesamiento paralelo pueden ser ventajosos. Además, la separación de varios componentes del sistema en los aspectos y ejemplos descritos anteriormente no debe entenderse que requiere tal separación en todos los aspectos y ejemplos, y debe entenderse que los componentes y sistemas del programa descritos generalmente pueden integrarse juntos en un solo producto de software o empaquetado en múltiples productos de software.

REIVINDICACIONES

1. Un método implementado por ordenador, que comprende:

i) extraer, en un dispositivo (302) de procesamiento, información (410) variable de datos (408) de registro de actividad de red que incluye una solicitud (402) de acceso al contenido de un usuario en una organización para una fuente (114, 116) de contenido de red;

ii) calificar (412) la información variable para generar una calificación (414) de riesgo que indica para la organización un riesgo relativo asociado con la fuente de contenido de la red;

iii) determinar (418) un nivel de control de acceso para la fuente de contenido de la red basado en la calificación de riesgo y una política (416) de acceso al contenido para la organización; y

iv) controlar (420) el acceso del usuario en la organización a la fuente de contenido de la red de acuerdo con el nivel de control de acceso, en donde la información variable incluye:

a) número (516) de veces que el contenido de la fuente de contenido de la red ha sido solicitado,

b) un volumen (518) de usuarios de la organización que han realizado una solicitud de contenido de la fuente de contenido de la red, y

c) un período (520) de tiempo para el que se ha detectado tráfico con respecto a la fuente de contenido de la red.

2. El método de la reivindicación 1, en el que la fuente de contenido de la red es un servidor (114) web que proporciona contenido web o una cuenta (116) de correo electrónico externa a la organización.

3. El método de cualquiera de las reivindicaciones 1 a 2, en el que la política (416) de acceso al contenido incluye un umbral de riesgo para la organización contra el cual se compara la calificación (414) de riesgo para determinar (418) el nivel de control de acceso.

4. El método de cualquiera de las reivindicaciones 1 a 3, en el que la calificación (414) de riesgo para la fuente (114,116) de contenido de la red es diferente en una segunda vez que es después de una primera vez que se determina (418) la calificación de riesgo para fuente de contenido de red.

5. El método de cualquiera de las reivindicaciones 1 a 4, que comprende, además:

i) formar los datos (406) de registro de actividad de la red utilizando la solicitud (402) de acceso al contenido del usuario en la organización.

6. El método de cualquiera de las reivindicaciones 1 a 5, en el que extraer (408) la información variable incluye:

i) clasificar (506) los datos del registro de actividad de la red en atributos (508,510,512) de datos, que incluye los datos del registro de actividad de la red:

(a) datos (502) de registro de actividad actual que comprenden la solicitud (402) de acceso al contenido del usuario en la organización y

(b) datos (504) de registro de actividad histórica que incluyen actividad previa para la red (112); y

(c) determinar (514) la información variable para la fuente de contenido de la red a partir de los atributos de datos.

7. El método de la reivindicación 6, en el que los atributos de los datos incluyen la identificación (508) de la fuente del contenido de la red, los nombres (510) de usuario de los usuarios de la organización en los datos del registro de actividad de la red y las horas y fechas (512) de acceso a la fuente (114,116) de contenido de red.

8. El método de cualquiera de las reivindicaciones 1 a 7, en el que controlar (420) el acceso del usuario en la organización a la fuente (114,116) de contenido de la red de acuerdo con el nivel (418) de control de acceso incluye permitir parte, pero no todo el contenido desde la fuente de contenido de la red para ser recibida por un dispositivo de la organización controlado por el usuario en la organización.

9. Un sistema que comprende:

i) un dispositivo (206) servidor que incluye:

a) un procesador (302); y

b) un medio (304) de almacenamiento legible por ordenador no transitorio que contiene instrucciones que, cuando se ejecutan en el procesador, hacen que el procesador realice el método de acuerdo con cualquiera de las reivindicaciones 1 a 8.

10. Un producto de programa informático incorporado de forma tangible en un medio (304) de almacenamiento legible por máquina no transitorio, que incluye instrucciones que, cuando son ejecutadas por un procesador de un aparato de procesamiento de datos, hacen que el aparato (206) de procesamiento de datos realice el método de cualquiera de las reivindicaciones 1 a 8.

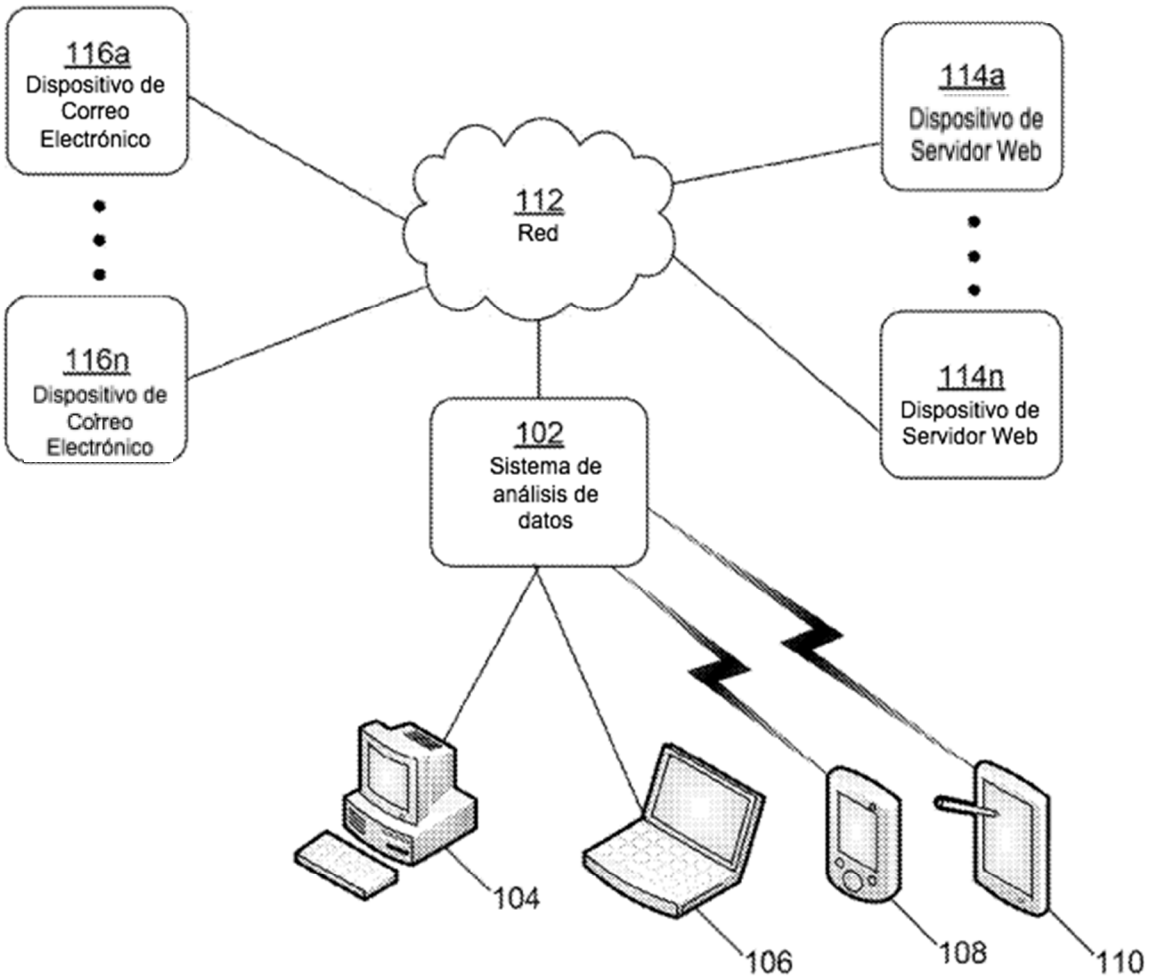
116a
Dispositivo de Correo Electrónico
116n
Dispositivo de Correo Electrónico
112
Red
114a
Dispositivo de Servidor Web
114n
Dispositivo de Servidor Web
102
Sistema de análisis de datos
104
106
108
110

FIG. 1

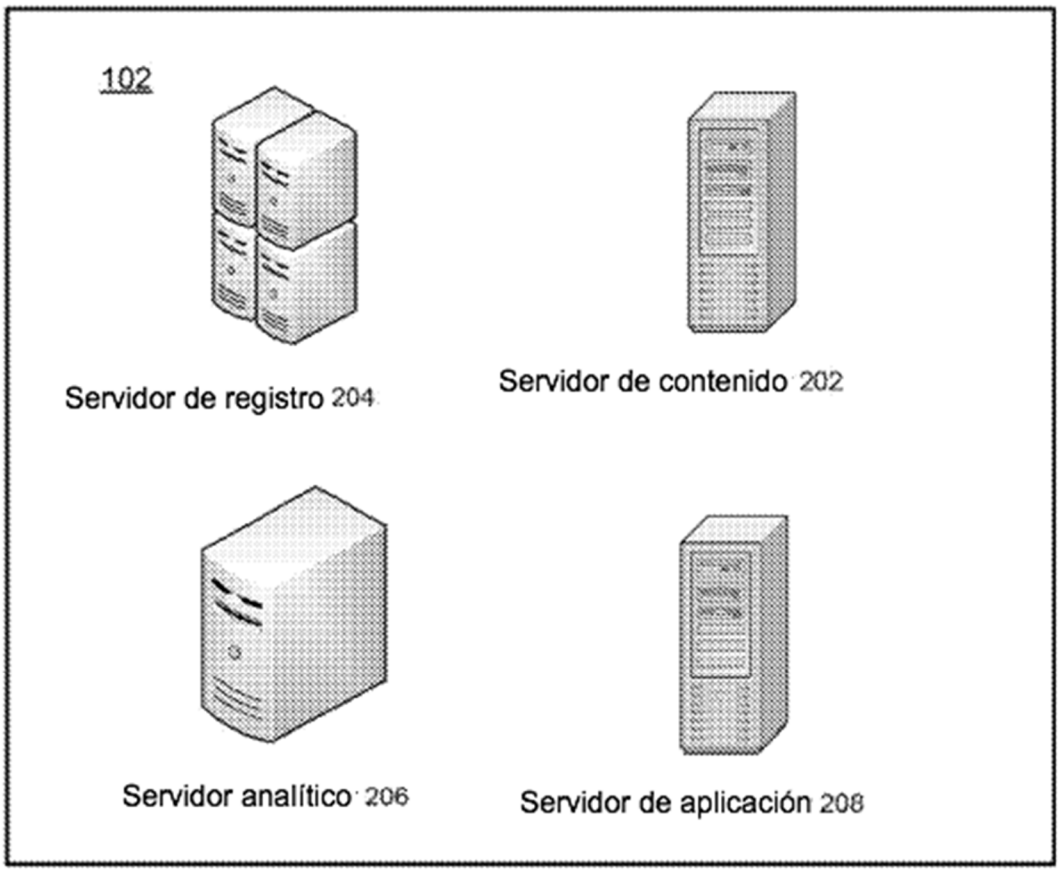
102
Servidor de registro 204
Servidor de contenido 202
Servidor analítico 206
Servidor de aplicación 208

FIG. 2

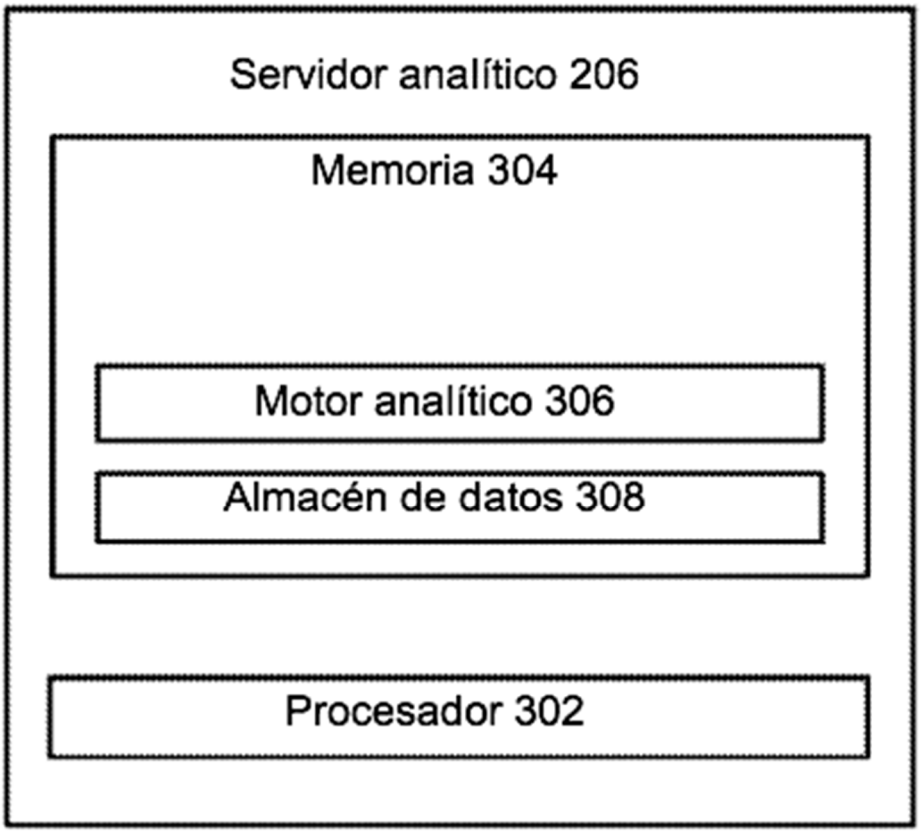
Servidor analítico 206
Memoria 304
Motor analítico 306
Almacén de datos 308
Procesador 302

FIG. 3

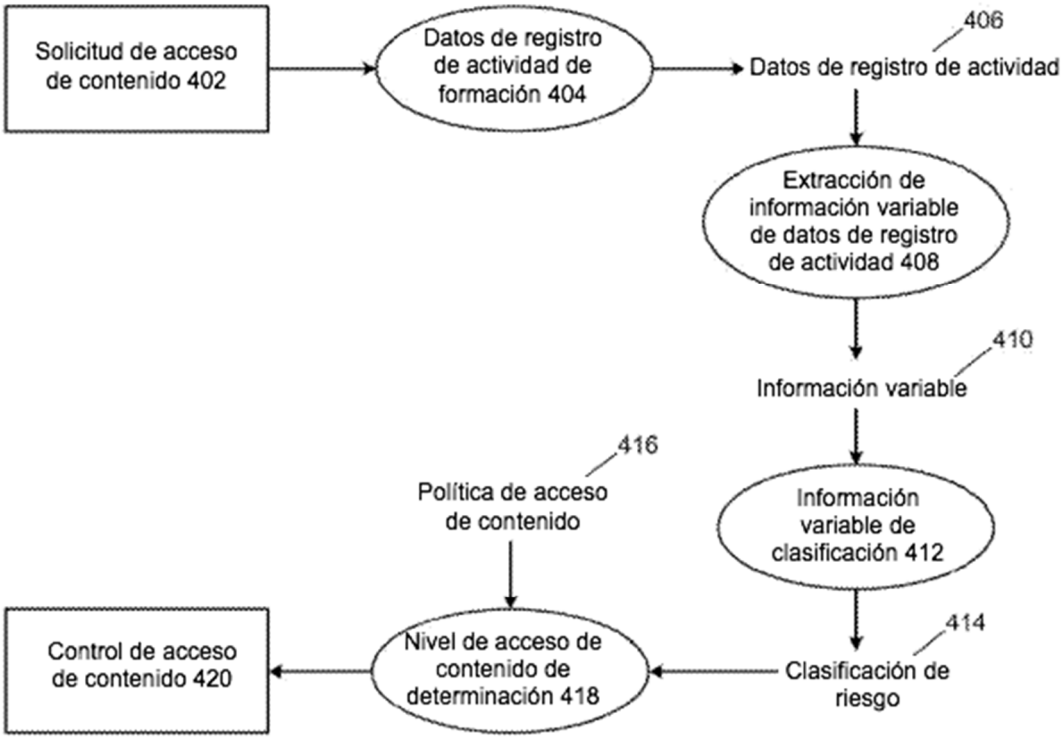
Solicitud de acceso de contenido 402
Datos de registro de actividad de formación 404
406
Datos de registro de actividad
Extracción de información variable de datos de registro de actividad 408
410
Información variable
416
Política de acceso de contenido
Información variable de clasificación 412
Control de acceso de contenido 420
Nivel de acceso de contenido de determinación 418
414
Clasificación de riesgo

FIG. 4

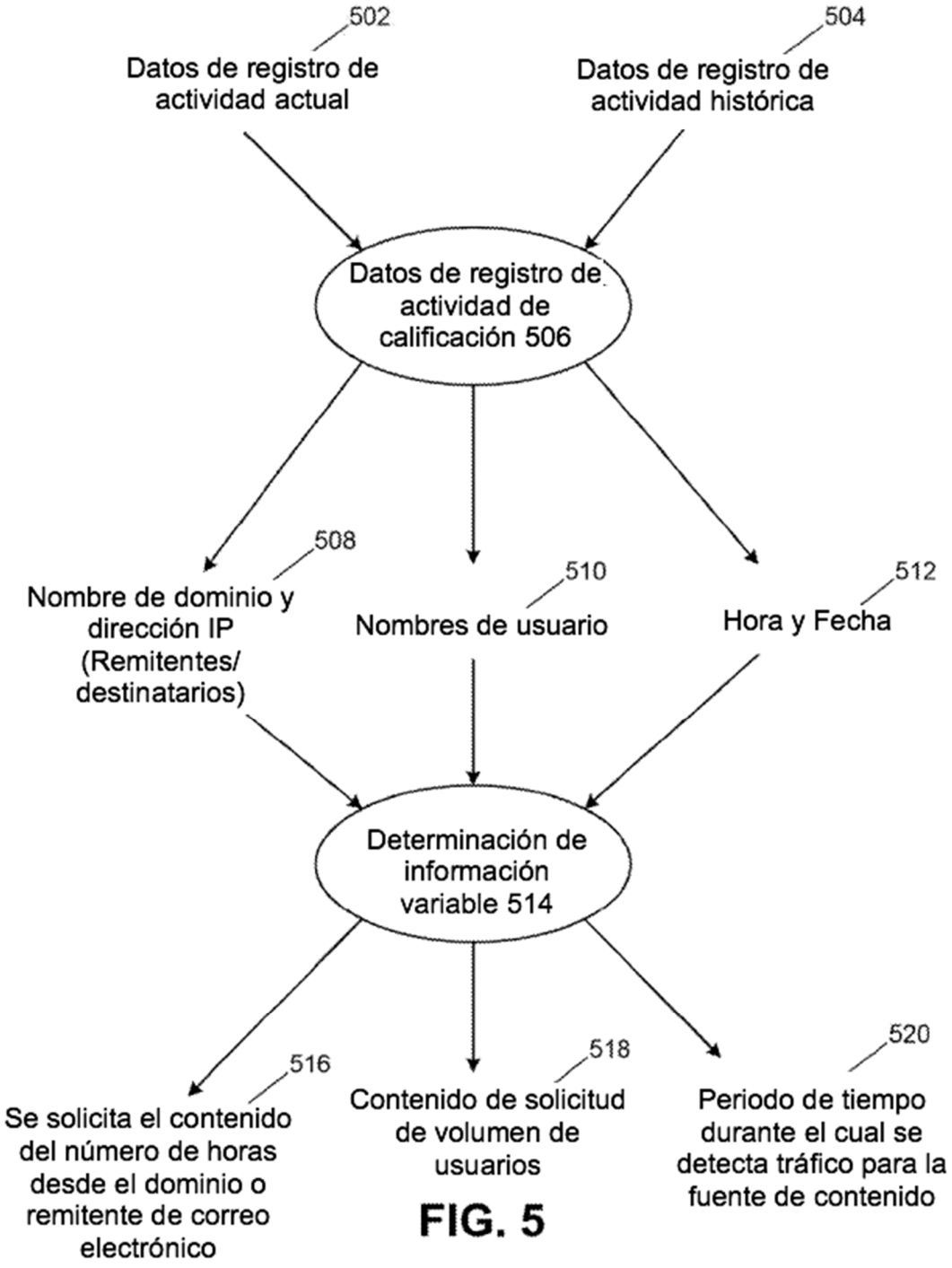
502
Datos de registro de actividad actual
504
Datos de registro de actividad histórica
Datos de registro de actividad de calificación 506
508
Nombre de dominio y dirección IP (Remitentes/ destinatarios)
510
Nombres de usuario
512
Hora y Fecha
Determinación de información variable 514
516
Se solicita el contenido del número de horas desde el dominio o remitente de correo electrónico
518
Contenido de solicitud de volumen de usuarios
520
Periodo de tiempo durante el cual se detecta tráfico para la fuente de contenido

FIG. 5

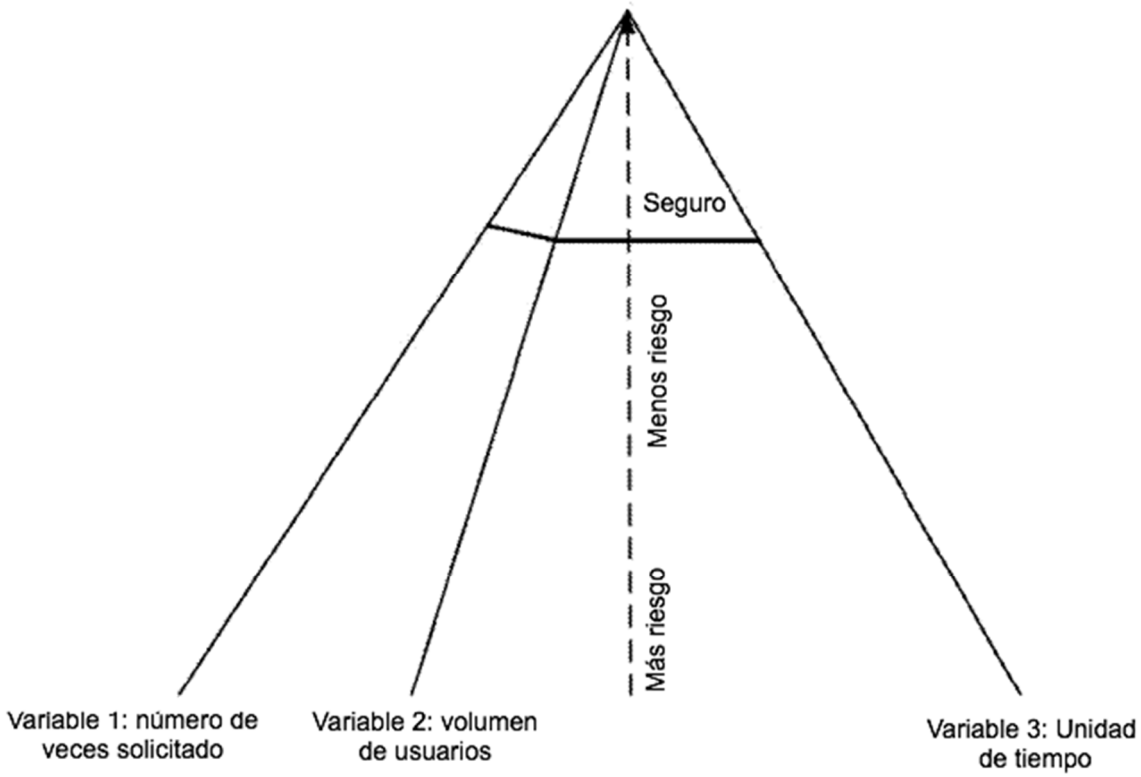
Seguro
Menos riesgo
Más riesgo
Variable 1: número de veces solicitado
Variable 2: volumen de usuarios
Variable 3: Unidad de tiempo

FIG. 6