(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 639 135**

(51) Int. CI.:

H04L 29/06 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **14.03.2013 E 13159266 (9)**

(97) Fecha y número de publicación de la concesión europea: **09.08.2017 EP 2677718**

(54) Título: **Autorización de fondo asincrónica secundaria (SABA)**

(30) Prioridad:

22.06.2012 US 201261663182 P
31.08.2012 US 201213600757

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
25.10.2017

(73) Titular/es:

IDECSI (100.0%)
21/23 Allee du Parc Garlande
92220 Bagneux, FR

(72) Inventor/es:

REZLAN, DANIEL;
COLLONGE, JEREMIE;
DUBROIS, LUC y
HUE, THIBAULT

(74) Agente/Representante:

SÁEZ MAESO, Ana

DESCRIPCIÓN

Autorización de fondo asincrónica secundaria (SABA)

Campo de la invención

La presente invención se refiere a sistemas y métodos (solución SABA) que monitorizan la confidencialidad de los recursos de TI del propietario, tal como correos electrónicos, acceso a su ordenador, acceso a sus archivos y problemas de fugas de datos. El sistema genera alertas al propietario cada vez que se compromete la confidencialidad. Este sistema aplica a análisis complejos y reglas de extrapolación para datos recolectados de muchas fuentes combinados con Geolocalización, recuperada de los dispositivos electrónicos.

Antecedente de la invención

Es conocido en la técnica de seguridad que todos los recursos individuales (es decir, buzones, dispositivos y datos sensibles) puedan ser accedidos fácilmente en cualquier tipo de arquitectura TI (es decir, auto hospedado, SaaS, Nube) y organización TI.

Técnicas populares en el arte para proteger el acceso a los datos incluyen las siguientes etapas:

1. Uso de una combinación de cuenta y contraseña para autenticar y recuperar credenciales que permiten el acceso a los recursos; y

2. Uso de un certificado personal para acceder a comunicaciones cifradas o almacenamiento.

Las técnicas recién descritas sufren de la desventaja de que en cualquier recurso de organización TI son:

- accedidas por el propietario,
- gestionadas por administradores de sistemas,
- accedidas por personas “confiables” (delegada) definidas por el propietario y/o el sistema administrador,
- guardadas en el disco o cinta por el administrador del sistema,
- protegidos por sistemas de seguridad de cuenta/contraseña que pueden ser hackeadas fácilmente,
- se pueden reenviar fácilmente correos electrónicos y datos a especialmente personas poco confiables.

Estas características se refieren a los servicios que se deben proporcionar mediante la organización TI con el fin de suministrar (i) continuidad comercial (ii) respaldo de datos y (iii) reparación de buzón. Por ejemplo, los administradores, por su función, deben tener derechos completos sobre los sistemas con el fin de ser capaces de tomar cualquier acción adecuada necesaria por los negocios o los usuarios. Más aún, los administradores tienen la capacidad de retirar todos los rastros de sus acciones.

Para superar este problema, la presente invención se ha diseñado para proteger a las personas y/o compañías de acceso indeseado a buzones, datos sensibles y recursos. Para proporcionar este servicio, la presente invención utiliza autenticación de fondo asincrónica secundaria (SABA) que es totalmente transparente y puede alertar al propietario de la información comprometida.

Resumen de la invención

Un objeto de la presente invención es proporcionar un sistema, basado en diferentes sistemas/software desarrollado en casa, que se aplica en el área de seguridad de datos para identificar amenazas en tiempo real, que incluyen, pero no limitan a robo de identidad, comunicación inapropiada a la competencia, acceso a datos no autorizados, y acceso físico no autorizado, y proporciona alerta a través de correo electrónico, SMS y llamadas telefónicas al propietario de la información. El sistema realiza una autorización de fondo secundaria que es transparente para que el solicitante verifique o indique un acceso no autorizado a los sistemas, datos u oficinas de la compañía que se solicitan. La autorización de fondo secundaria se basa en un método de modelado de gran coincidencia de patrones de datos, y seguridad privada, hecho posible mediante la creación, expansión y análisis de nuevos “flujos de datos” que, junto con los Sistemas Operativos, aplicaciones y datos de dispositivos, permiten únicamente al sistema determinar un riesgo de acceso de seguridad y proporcionar información al usuario afectado.

De acuerdo con un aspecto de la presente invención, se proporciona un módulo con agentes en tiempo real para crear, recolectar y almacenar Perfiles de Autorización de propietario para todos los propietarios y delegados. Un delegado

puede ser cualquier persona que el propietario identifica al sistema como permitido para acceder a la información del propietario.

De acuerdo con otro aspecto de la presente invención, un propietario es la persona que posee la información, por ejemplo, datos, documentos, correo electrónico, correo de voz, etcétera. El sistema SABA protege la información del propietario.

De acuerdo con otro aspecto de la presente invención, un delegado es una persona que tiene acceso autorizado a la información del propietario. Por ejemplo, una secretaria puede tener acceso al correo electrónico del Director Ejecutivo, a discreción del Director Ejecutivo. La secretaria es una delegada del Director Ejecutivo. Esta distinción evita enviar una alerta al propietario cada vez que su secretaria lee su correo electrónico.

De acuerdo con otro aspecto de la presente invención, se proporciona un módulo con agentes en tiempo real para recuperar la identidad teórica del usuario que tiene acceso a los recursos del propietario ("el solicitante"). Estos agentes también recolectan toda la información de perfil disponible con respecto al solicitante al momento de la solicitud.

De acuerdo con otro aspecto de la presente invención, un solicitante es una persona que intenta tener acceso a la información del propietario. El sistema SABA analiza la identidad del solicitante para definir si él es un propietario o un delegado. Si no es ninguno, el sistema SABA envía alertas a una persona designada quien puede ser el propietario o una persona designada (es decir, Gerente de Seguridad).

De acuerdo con otro aspecto de la presente invención, una persona designada o usuario designado es una persona que esta designada para manejar el sistema SABA para la compañía personalizada o para recibir alertas.

De acuerdo con el sistema de SABA la invención, los usuarios incluyen propietarios, delegados y solicitantes. En un sistema de información de compañía, un usuario puede ser cualquier empleado, o cualquier no empleado que tiene acceso o intenta tener acceso a información almacenada en el sistema.

De acuerdo con otro aspecto de la invención, un Personal Autorizado es una persona que tiene acceso a recursos de sistema de información de la compañía independientemente del sistema SABA. El Personal Autorizado frecuentemente son administradores del sistema.

De acuerdo con otro aspecto de la invención, un usuario monitorizado es cualquier usuario que intenta acceder a información protegida. Un solicitante se convierte automáticamente en un usuario monitorizado en el momento que el solicitante busca acceder a la información protegida. De acuerdo con la realización preferida de la invención, el sistema determina si el usuario solicitante/monitorizado es un propietario, un delegado o un usuario no autorizado.

De acuerdo con otro aspecto de la presente invención, se proporcionan agentes de Geolocalización de solicitante en tiempo real.

De acuerdo con otro aspecto de la presente invención, se proporcionan agentes de Geolocalización de propietarios o delegados en tiempo real.

De acuerdo con otro aspecto de la presente invención, se proporcionan Programas y Reglas Complejas para analizar y comparar datos extrapolados (perfiles y Geolocalización) del solicitante, propietario o delegado. Estos programas identifican los intentos de fraude.

De acuerdo con otro aspecto de la presente invención, se proporciona un sistema de alerta que envía alertas utilizando cualquier servicio de comunicación como clientes de correo electrónico, SMS y teléfonos inteligentes para informar al propietario de una ruptura de la confidencialidad. También está disponible una interfaz de seguridad basada en red dedicada para gestión de historial e informes

De acuerdo con otro aspecto de la presente invención, se proporciona una configuración, administración y visualización de información de sitio web.

De acuerdo con otro aspecto de la presente invención, el sistema puede proporcionar opcionalmente mecanismos para bloquear el acceso a recursos en situaciones cuestionables con un método para que el usuario autentique su identidad con el fin de proceder.

Descripción de los dibujos

La posterior descripción de las realizaciones preferidas de la presente invención se refiere a los dibujos adjuntos, en los que:

La figura 1 describe un entorno de usuario típico en sistemas de empresa o servicios de nube;

La figura 2 describe entornos de usuario típico en sistemas empresariales o servicios de nube con el sistema SABA;

La figura 3 describe la arquitectura general de un sistema de autenticación de fondo asincrónico secundario (“SABA”);

La figura 4 describe sistemas de colector PADO;

La figura 5 describe un recuperador de identidad SABA;

La figura 6 describe módulos de Geolocalización SABA;

La figura 7 describe sistema de extrapolación y análisis SABA;

La figura 8 describe procesos de verificación de identidad SABA genéricos (buzón o cuenta);

La figura 9 describe procesos de protección de respaldo SABA; y

La figura 10 describe procesos de protección de fuga de datos SABA.

Descripción detallada de la invención

En la siguiente descripción, se establecen diversos detalles para proporcionar una explicación más a fondo de la presente invención. Sin embargo, será evidente para el experto en la técnica, que la presente invención se puede practicar sin estos detalles específicos. En otros casos, los dispositivos y estructuras bien conocidos se muestran en forma de diagrama de bloques a diferencia de en detalle, con el fin de evitar oscurecer la presente invención.

La figura 1 es un ejemplo de la arquitectura de un entorno TI típico, que incluye tanto Hardware (es decir, servidores, PC, almacenamiento equipos de red, equipos de seguridad, etcétera) y Software (es decir, sistemas operativos, mensajería, aplicaciones de usuario, etc.).

Muchas compañías albergan este tipo de sistema en las instalaciones (100), pero con la expansión del internet y la computación (101) en nube están empezando a externalizar sus recursos y sus datos. Usualmente en una compañía existen servidores para el sistema de mensajería, un sistema de procesamiento de llamadas, servidores de archivos, servidores de aplicaciones, servidores de base de datos y servidores de administración.

Normalmente existen dos tipos de servidores PBX (102), tradicional e IP. El software de procesamiento de llamadas se instala normalmente en ese servidor y se utiliza para manejar todas las llamadas entrantes y salientes de la compañía.

El software de mensajería se instalará usualmente en el servidor (103) de correo para manejar los buzones de los usuarios, así como enviar y recibir correo de los usuarios.

Están disponibles diferentes tipos de servidor (104) de archivos. Un servidor independiente tradicional o grupo con almacenamiento unido puede manejar esta funcionalidad. Normalmente esto es lo que hará un NAS. Los usuarios almacenarán documentos sobre el servidor de archivo para acceder/utilizar por ese usuario y para compartir con otros usuarios.

Un sistema de gestión de base de datos relacionales tal como Microsoft SQL Server, Oracle, Mysql, Postgress se instalará en el servidor (105) de base de datos. Usualmente se conectará a un sistema de almacenamiento y se utilizará para almacenar y manipular una gran cantidad de datos.

El servidor (106) de aplicación se puede ser instalar como una aplicación orientada al usuario que se puede utilizar para contabilidad, recursos humanos, inteligencia comercial, ventas, etcétera.

Un servidor (107) de Acceso de Seguridad se puede utilizar para controlar acceso autorizado a las diferentes ubicaciones en la empresa. Por ejemplo, para ir a la sala de archivo financiero, un usuario tendrá que utilizar una insignia que se programa mediante este sistema, y cuando él tiene acceso a esta sala el sistema lo registra.

Los servidores (108) de administración se pueden utilizar para gestionar otros sistemas, así como a los usuarios o los recursos de la compañía. El sistema de gestión de software se instalará en ese servidor permitiendo al administrador gestionar todos los recursos desde un punto centralizado.

Todos los servidores de una compañía se pueden vincular por y acceder a través de una red. La mayor parte del tiempo, el trabajo en red también permitirá conexiones externas de tal manera que los usuarios pueden acceder a recursos externos en internet o acceder a los recursos de la compañía desde internet. La red se basa en equipos de red tal como enrutadores o conmutadores. Para ser capaces de enrutar la información al destino correcto, el equipo de red utilizará TCP/IP.

Basado en el tipo de comunicación utilizada por los usuarios, se utilizarán otros protocolos (es decir, SMTP, HTTP, FTP, SNMP). Dichos protocolos tienen la opción de ser asegurado. Cuando estos protocolos se aseguran toman una "s" (por ejemplo: HTTPs).

Esta red también permite a los usuarios de la compañía intercambiar datos e información con personas externas de otras compañías que utilizan sistemas de correo u otros sistemas tal como servidores de transferencia de archivos.

Los servidores por sí mismos se pueden unir a sistemas de almacenamiento ya sea unido directamente al servidor (SCSI) o a través de la red (SAN, NAS). Estos sistemas de almacenamiento permiten que se almacenen un enorme volumen de datos.

Los sistemas ahora también pueden ser accedidos a través de dispositivos (109) móviles tal como teléfonos inteligentes, ordenadores tipo tabletas y ordenadores portátiles. Estos dispositivos se pueden proporcionar por la compañía o por el usuario propiamente dicho. Estos dispositivos se utilizan frecuentemente para enviar y recibir correo electrónico o para transferir datos. También se pueden utilizar para acceder a los recursos de la compañía. Ahora se ha vuelto posible para un usuario trabajar desde cualquier ubicación como si estuviera en su oficina.

Para proteger los datos del exterior, o para controlar lo que un usuario puede hacer con los datos, las compañías han implementado sistemas de seguridad como Firewalls, servidores proxy y VPN segura (110).

Se ha vuelto más fácil para los usuarios, debido a la tecnología, intercambiar información con personas dentro o fuera de la compañía. También se ha vuelto más fácil para los usuarios almacenar una gran cantidad de datos en sus dispositivos personales.

Al mismo tiempo se ha hecho más difícil gestionar todos los recursos del sistema de información. Por esa razón, se han implementado servidores centralizados para administración. Estos servidores son manejados por personas especializadas quienes manejan tareas como gestión de usuario, gestión de hardware, gestión de red, asignación de recursos y gestión de derechos.

En razón a esa complejidad y ese poder sobre los sistemas, se han implementado sistemas (111) de seguimiento de recursos de registro en la compañía. Hoy en día todas las acciones tomadas sobre un sistema, tal como crear un nuevo usuario, asignación de derechos, creación o supresión de datos, acceso a la información, o modificación de configuración del sistema, son registrados en los sistemas de seguimiento de registro.

Será más difícil para la compañía conservar el control de sus datos cuando el sistema de información de la compañía se aloja fuera de la compañía dentro de una compañía SaaS o en la nube. Luego se volverá crítico para la compañía que todas las acciones tomadas sobre datos o sobre los sistemas sean rastreadas.

La arquitectura de un entorno TI con un sistema SABA de acuerdo con la presente invención, como se ve en la figura 2, muestra una implementación global del sistema SABA.

El sistema SABA de la presente invención es una solución integrada basada en diferentes módulos:

1. La Gestión del Sistema Central (CSM) (200) que es el núcleo del sistema. El CSM (200) incluye preferiblemente pero no se restringe a,

a. Motor Recolector (CE) (201): Este sistema recolecta preferiblemente y analiza los datos técnicos enviados por el LEM (206) y el GEM (207) antes de transferirlo a un AES (203) utilizando el colector PADO, recuperador TADR o colector de Geolocalización.

b. Sistemas de Geolocalización (GS) (202): Este sistema geocodifica preferentemente los recursos de usuarios monitorizados (solicitantes, propietarios y delegados) a través de bases de datos dedicadas y proveedores (208) de geocodificación.

c. Sistemas de Análisis y extrapolación (AES) (203): Estos sistemas almacenan preferentemente y analizan datos recolectados del solicitante, propietario y recursos delegados y sistemas,

d. Sitio Web de Gestión y Configuración (MCWS) (204): Este sistema permite preferiblemente que la configuración del sistema SABA y la visualización de datos para usuarios monitorizados.

e. Sistemas de alerta (AS) (205): Este sistema envía preferiblemente alertas a usuarios monitorizados después de ser procesados mediante sistemas de análisis y extrapolación.

2. Módulo de Extracción Local SABA (LEM) (206): Este módulo puede ser hardware, software o una combinación de ambos. Un dispositivo de hardware puede incluir un procesador de sistema, algo de memoria volátil como RAM y un

sistema de almacenamiento local tal como una unidad física para almacenar temporalmente datos recolectados. El software de SABA LEM puede incluir un software de sistema operativo, así como software específico de SABA. El SABA LEM (206) recolecta datos de diversos sistemas y recursos. Los datos recolectados son registros que incluyen información relacionada con el usuario monitorizado, así como información proporcionada por agentes relacionados con recursos monitorizados. Aquellos registros se recolectan de Servidores de Correo, Servidores de Archivos, Equipos de Red, Equipos de Seguridad, PBX/IP PBX, Servidores de Administración, etcétera, (212). Los datos recolectados son enviados por agentes relacionados con los sistemas monitorizados al Motor Recolector (201).

3. Módulo de Extracción de Geolocalización SABA (GEM) (207): Esto incluye Software para rastreo de datos relacionados con Geolocalización de dispositivos de usuarios monitorizados y enviados al sistema (202) de Geolocalización a través del recolector de Geolocalización.

El sistema SABA se basa en dos grupos principales de datos. La Solicitud de Datos de Autenticación Teórica (TADR) (209), almacena todos los datos no verificados de un solicitante y los datos de Autenticación Personal del Propietario (PADO) (210), almacena todos los datos certificados de los propietarios. Opcionalmente, el PADO también almacena todos los datos certificados de delegados.

Cuando se instala SABA, se realizará comprobación de fondo para verificar que el solicitante de un recurso monitorizado es realmente quien dice ser.

Cada acción llevada a cabo por un solicitante en un Recurso Monitorizado, desde el interior o desde un entorno (211) externo y/o móvil se envía al AES (203) a través del Motor Recolector (201) utilizando SABA LEM (206). Esta información se define como TADR (209).

Cada acción llevada a cabo por un propietario (y, opcionalmente, delegados) sobre un recurso monitorizado, desde dentro o desde un entorno (211) externo y/o móvil, es enviado a los sistemas de análisis y extrapolación (203) a través del Motor (201) Recolector utilizando SABA LEM (módulo de extracción Local) (206) y los sistemas (202) de Geolocalización, que incluye SABA GEM (módulo de extracción de Geolocalización) (207). Esta información se define como PADO (Datos de autenticación Personal del propietario) (210).

Los AES (sistemas de análisis y extrapolación) (203) compararán el TADR (209) con PADO (210) para definir si se inicia la acción por el propietario o un delegado, o por un ladrón. Para hacer esta determinación, el AES (203) aplica una serie de reglas que utilizan información en tiempo real o información pre calculada específica para cada usuario monitorizado.

Si el resultado no coincide no valida el TADR (209), se envía una alerta a uno o más dispositivos del propietario o delegado (213) utilizando sistemas de alertas (AS) (205).

Cuando se recibe una alerta, el propietario tendrá que conectar el sistema SABA para confirmar si la alerta es legítima o no. Esto permitirá al PADO refinar la información autorizada/monitorizada de los usuarios y su uso.

El Segundo Sistema de Autenticación de Fondo Asincrónico muestra cómo una realización de la figura 3 como el sistema SABA puede ser gestionado, configurado y cargado utilizando el sistema de configuración y gestión SABA, el Sistema de Alerta y el Sitio de Red de Alerta.

El sistema de configuración y gestión (300) SABA permite la configuración del Motor (318) Recolector (que incluye recuperador de identidad de información (304), recolectores (305) PADO y Geolocalización (309) PADO, procesadores (308) de flujo de datos SABA y sistemas de alertas (301).

Los sistemas (301) de alerta envían alertas a los usuarios monitorizados. Este sistema también validará información del TADR que se va a transferir al PADO del usuario una vez se ha certificado la información por el propietario.

El Sitio (302) de Red de Alerta es para observar alertas archivadas y reconocer nuevas alertas.

El sitio web (313) de configuración y gestión SABA y el sistema (300) permiten a los administradores SABA manejar (crear, modificar, suprimir, visualizar) propietarios, y delegados y Sistemas Protegidos. Estos módulos pueden configurar y almacenar información con respecto a los propietarios y delegados (nombre de usuario, primer nombre, apellido, dirección de correo, ID de dispositivos, direcciones personales y de oficina, etc.), sistemas (nombres de host URI, puertos, dominio, etc.) y reglas de alerta (horas de hábiles de propietario y delegados, tipo de acceso, etc.) con el fin de que el sistema SABA sepa qué recursos se tienen que proteger y qué propietarios y delegados se tienen que monitorizar.

También se crea un PADO personal y único asociado a un propietario. El PADO recibe dos tipos de información: información de actividad de propietario e información de Geolocalización de propietario. Estos dos tipos de información permitirán al sistema SABA certificar la identidad del propietario.

El sistema SABA empezará a registrar toda la información recuperada de las acciones del propietario en su PADO, utilizando el recolector (305) SABA PADO para analizar y clasificar todos los datos técnicos emitidos de los agentes instalados en las aplicaciones, sistemas y dispositivos monitorizados de delegados y propietarios.

Un usuario siempre tiene acceso o hace una acción en un Sistema Protegido utilizando un ID (Cuenta, Insignia, etcétera). El sistema SABA considera a este usuario como un solicitante ("solicitante") con una identidad teórica que se tiene que validar como se describe adelante.

Utilizando datos de configuración, el sistema SABA monitoriza los sistemas (307) protegidos a través del Recuperador de Identidad Teórico (TIR) (304) que recolecta información de registro enviada por el LEM y transfiere esta información a Procesadores de Flujo de Datos (DSP) (308) para tratamiento.

El DSP (308) almacena esta información en una base de datos temporal, identifica el tipo de información con el Procesador de Análisis de Tipo (315) y publica a procesadores (314) de flujos de datos TADR, que han sido suscritos previamente con este tipo de información, de que un nuevo evento está disponible. Los procesadores (314) de flujo de datos TADR solicitan a la base de datos temporal recuperar la identidad del solicitante y toda la información disponible acerca del solicitante, carga el almacén (306) de datos TADR y lanza el Procesador (316) de Reglas Funcionales y de Extrapolación para tratamientos.

Procesadores de Análisis de Tipo (315), que dependen del tipo de información, proporciona un grupo de datos TADR a procesadores (316) de reglas funcionales y de extrapolación que ejecutan diferentes reglas para comparar con los datos TADR establecidos para:

(i) el perfil de usuario monitorizado, almacenado en el almacén (303) de datos PADO,

(ii) los datos de Autenticación Personal para Geolocalización (312), de Propietario, recuperadas de Geolocalización (309) PADO. Estos datos se han geocodificado previamente utilizando proveedores (310) de geocodificación que incluyen, pero no se limitan a Google, Bing y Yahoo.

Si los datos no se validan por el SABA DSP, se enviará una alerta al propietario o a una Persona Designada que utiliza el sistema (301) de alerta. El propietario entonces tendrá que confirmar si él o un delegado es el que realiza la acción en el Sistema Protegido. Si el sistema de SABA recibe la confirmación a través del Sistema de Alerta o el Sitio de Red de Alerta de que la acción ha sido tomada por el propietario, entonces cargará al PADO con nueva información.

En la figura 4 se describen los Agentes recolectores de Diferentes Datos de Autenticación Personal del Propietario (PADO)

A saber, por ejemplo:

- Cuál es el hardware utilizado por un propietario,

Cuál es el tipo de sistema operativo que está instalado,

Qué tipos de aplicaciones de software son utilizadas frecuentemente por un propietario,

Qué tipo de red es la que conecta el hardware,

En dónde se ubica esa red,

En dónde está ubicado el propietario,

Qué está haciendo el propietario,

El sistema SABA puede recuperar la información con respecto al propietario y el almacenamiento de esta información en el PADO del propietario. Para recolectar esta información, el sistema SABA proporciona recolectores SABA PADO (400) que recuperan y clasifican datos técnicos enviados por un grupo de agentes PADO (programas que recuperan información acerca de acciones y conexiones de un propietario identificado de diferentes fuentes) instalado en dispositivos de usuario monitorizados, aplicaciones, que incluyen Sistemas Protegidos y que son sistemas relevantes.

Cada agente envía actividades de usuario monitorizadas para SABA LEM que lo transfiere a los Recolectores PADO o directamente a los Recolectores PADO dependiendo de la ubicación del dispositivo.

Los agentes incluyen, pero no se restringen a, agente PBX (401), agente (402) de acceso físico, agente (403) de información de red, agente (404) de información de dispositivo, agente (405) de información de aplicación de software, y agentes (406) de credenciales. Los agentes capturan información o la recolectan de datos directamente disponibles de sistemas o registros.

El agente PBX recupera llamadas entrantes o salientes del PBX/IP PBX (407) para validar la presencia física del usuario en su oficina. Es igual con el Agente de Acceso Físico que obtiene una información (408) de tarjeta/insignia.

Un agente (403) de información de red define una identificación y ubicación de dispositivo.

El agente (404) de información de dispositivo de propietario recupera información tal como qué tipo de hardware se está utilizando, y qué tipo de sistema operativo está instalado, qué aplicaciones se utilizan frecuentemente. Este agente se instala en dispositivos (411) de usuario monitorizados.

El agente (405) de aplicaciones de propietario recupera información como qué aplicaciones se están utilizando frecuentemente. Este Agente se instala en los dispositivos (411) de usuario monitorizados.

Toda la información recolectada se transferirá al SABA LEM y luego al recolector PADO o directamente al recolector PADO. Desde allí, esta información se analizará y clasificará para definir qué datos técnicos corresponden a las acciones del propietario validadas. Luego, la información se transfiere al procesador PADO DataStream y se almacena en el almacén de datos PADO. Toda la información recolectada se utilizará con el fin de construir el perfil de usuario.

La información recolectada acerca de la aplicación utilizada, llamadas, etcétera ayudará a definir el comportamiento del usuario monitorizado (por ejemplo: el usuario llega todas las mañanas a las 10 de la mañana, siempre se registra y luego inicia el software de correo corporativo. Él hace una llamada antes de inicializar su explorador de red. El explorador de red utilizado siempre es IE v9).

La figura 5 ilustra una realización de los Agentes Recolectores Recuperadores de Identidad de Solicitante Teóricos.

Los recuperadores de identidad teóricos (TIR) SABA (500) reciben y clasifican datos técnicos enviados por un grupo de agentes TIR (programas que recuperan información acerca de nuevas conexiones o acciones realizadas sobre sistemas protegidos que se tienen que validar, desde diferentes fuentes) instalado en todos los sistemas protegidos. Una vez recolectado por el SABA LEM, esta información se transferirá al Recuperador de Identidad Teórico SABA en el Motor Recolector. Cuando se recibe por el SABA TIR, la información se analizará y filtrará para identificar una nueva conexión o una nueva acción sobre los sistemas protegidos y luego se enviará la información al procesador de flujo de datos SABA TADR que lo almacenará en la Solicitud de Datos de Autenticación Teóricos (TADR). El SABA TIRA se desarrolla en casa para asegurar que la información se recupera en forma segura desde los sistemas. El SABA TIRA se activa automáticamente tan pronto como se tiene acceso a datos, o dispositivos del Sistema Protegido.

Los Sistemas Protegidos son sistemas o datos declarados como sensibles por el propietario en un sistema SABA, utilizando la configuración SABA y el Sitio de Red de Gestión. Pueden incluir sistemas de buzón, aplicaciones críticas, sistemas de respaldo y problemas de Fugas de Datos. Se dividen en 4 categorías principales:

- Revisión de identidad de cuenta (501),

Revisión de identidad de correo (502),

Revisión de ID de respaldo (503)

Revisión de fuga de datos (504).

La verificación (501) de identidad de cuenta se basa en un grupo de SABA TIRA. La función de estos agentes es recuperar el ID de solicitante de todo tipo de software o hardware que solicita una identificación, tal como las aplicaciones (505), sistemas (506) operativos, accesos de red (VPN) (507), accesos de software de control (508), software de seguridad y proporcionar todos los datos asociados.

El SABA TIRA se puede instalar en servidores, PC, dispositivos móviles, accesorios, equipos de red.

Para revisión (501) de identidad de cuenta existe un agente específico para cada tipo de sistemas accedidos con credenciales específicas:

- Agente dedicado de aplicación (509)
- Agente dedicado OS (510)
- Agente dedicado de red VPN (511)
- Agente dedicado de seguridad de acceso (512)

La revisión de identidad de correo (502) se basa en 2 tipos de agentes SABA TIRA que monitorizarán cualquier acción tomada en un buzón monitorizado. SABA TIRA se instalará en los sistemas de correo y recupera información de acceso, derechos de auditoría y el tipo de acciones hechos en el buzón del propietario. Estos dos Agentes de Comprobación de Identidad de Correo son:

- Agente de sistema de correo SABA (513)

Agente Blackberry SABA (514)

La comprobación de ID de respaldo (503) se basa en dos SABA TIRA que:

- crearán un sistema de archivos seguro para datos de respaldo, y
- seguimiento de todas las modificaciones de archivos.

Los archivos de respaldo o datos serán “marcados” y sólo se pueden restaurar dentro de un Sistema Protegido. Estos agentes son:

- almacenamiento dedicado SABA (516)
- agente dedicado de auditoria de Archivos (515)

La comprobación (504) de fuga de datos se basa en SABA TIRA. Estos agentes recolectan datos de sistemas de correo, PBX/IP PBX, servidores de impresión, etcétera. Una vez se recolectan los datos, se enviarán al SABA TIR a través del SABA LEM y luego se transferirán al AES para ser comparados contra una lista de palabras clave. Las palabras, números telefónicos, direcciones de contacto (correos electrónicos) se definen por el propietario, por ejemplo, la competencia, proyectos secretos, caza talentos, etcétera.

estos agentes son:

- Agente recuperador de nombre de dominio SABA (517), utilizado para registrar el receptor de todas las comunicaciones numéricas salientes como mensajería instantánea, correos, etcétera.
- Agente recuperador de llamadas SABA (518), utilizado para recuperar información de registros de PBX/IPBX y recolectar todos los números de llamadas entrantes/salientes y contactos asociados.
- Agente (519) recuperador SABA Print, utilizado para conseguir el nombre de los documentos impresos.

En la figura 6 se describen Agentes Recolectores de Geolocalización.

Los agentes recolectores de Geolocalización SABA (GCA) (600) se instalan en los recursos o dispositivos móviles del propietario y delegados. Dependiendo del tipo de agente, la información recolectada se enviará al SABA GEM que la transferirá al Recolector de Geolocalización de Actividad SABA o directamente al Sistema de Geolocalización SABA ubicado en SABA AES. Cuando es recibido por el SABA AES, esa información se almacenará en los Datos de Autenticación Personal para el Propietario (PADO) mediante los procesadores de flujos de datos SABA PADO. Los agentes recolectores de Geolocalización SABA (GCA) se desarrollan en casa para asegurar que la información se recupera en forma segura desde los sistemas. El SABA GCA se activa permanentemente.

El Recolector de Geolocalización SABA (600) se divide en dos tipos de Recolectores:

- Geolocalización de Actividad (601)
- Geolocalización de Dispositivo (602)

El recolector (601) de Geolocalización de actividad recupera, de diferentes agentes recolectores, la información relacionada con Geolocalización de todos los eventos relacionados generados por la actividad del usuario y los correlaciona con datos ya almacenados en PADO. Todos los agentes recolectores envían datos técnicos al GEM que los transfiere al recolector de Geolocalización de actividad en el motor recolector. Por ejemplo del Agente Recolector PBX (603), el sistema puede deducir si el usuario monitorizado está utilizando su teléfono en su oficina; desde el Agente Recolector de Rastreo de Ordenador (605), el sistema puede saber que el usuario monitorizado está en su oficina utilizando su ordenador y recuperando su posición; desde el agente recolector de presencia (606), el sistema obtiene inmediatamente el estado de su localización; desde agente (607) recolector de calendario, el sistema puede saber su agenda y localización; desde los agentes recolectores de pago (608), el sistema sabe el lugar donde se hace la transacción y se deduce la posición de usuario monitorizada.

Los Recolectores de Geolocalización de Dispositivo (602) recuperan, de diferentes agentes recolectores, la información relacionada con Geolocalización del dispositivo móvil del propietario y delegados o posiciones de elementos de red. El Recolector de Geolocalización de Dispositivo (602) recupera datos técnicos de dos tipos de agentes:

- El Agente Recolector de Geolocalización de Móviles (610) instalado en el dispositivo del propietario y los delegados, que consigue en forma precisa el posicionamiento geográfico de triangulación GPS o GSM. La información recolectada por este agente se envía al módulo Extractor de Geolocalización (GEM) y se transfiere al recolector de Geolocalización de dispositivo;

- Agente Recolector de Geolocalización de Red (609), que consigue dirección IP o punto WIFI utilizado por el propietario y el delegado. La información recolectada por este agente se envía al módulo Extractor de Geolocalización (GEM) y se transfiere al recolector de Geolocalización de dispositivo;

Los Análisis SABA y El Sistema de Extrapolación se describen en la figura 7.

El sistema de extrapolación y análisis SABA (AES) (700) es el núcleo del sistema SABA. El AES es el módulo que almacena, recupera, manipula y ejecuta las reglas funcionales y de extrapolación (701) sobre TADR (705) PADO (706) y datos (711) de Geolocalización para definir si el solicitante (que utiliza ID de solicitante (714)) es quien dice ser. Para hacer eso, el AES utilizará:

- toda la información del propietario y delegado almacenada en el PADO,

- toda la información del solicitante almacenada en TADR,

- la Geolocalización de delegado y propietario basada en su actividad y/o en sus dispositivos, calculado mediante los sistemas de Geolocalización SABA (715).

El Procesador de Flujo de Datos PADO (713) es un módulo construido con los perfiles de propietario y delegado, basado en información recolectada por los agentes recolectores SABA y enviado por el SABA LEM, información de Geolocalización basada en datos recolectados del sistema de Geolocalización SABA (715) o datos llenados por el propietario directamente a través del Sitio Web de Configuración y Gestión (MCWS).

El PADO (706) es un Almacén de Datos que contiene toda la información verificada disponible acerca del propietario y delegados. El PADO contiene:

- Usos (707) de usuario hechos de:

  - Usos de trabajo (708)

  - Usos de dispositivo (709)

  - Usos de aplicación (710)

- Geolocalización de usuario definida a partir de actividad y dispositivos (711).

El Procesador de Flujo de Datos TADR (712) es un módulo que construye el perfil del solicitante, basado en información recolectada por los Agentes de Recuperación de Identidad Teórica SABA, enviado por el SABA LEM y almacenado en el grupo de datos TADR (705).

El procesador de análisis tipo SABA (702), que depende del tipo de información, proporciona el grupo de datos TADR para los Procesadores de Reglas Funcionales y Extrapolación (701). Dependiendo del resultado, este módulo solicita al Sistema de Alertas (704) enviar alertas.

El procesador de reglas funcionales y extrapolación (701) ejecuta diferentes reglas para comparar el grupo de datos TADR con:

(i) el perfil de usuario monitorizado, almacenado en el almacén de datos PADO (706)

Los datos de autenticación personal para la Geolocalización del propietario (711) recuperada de agentes de Geolocalización PADO (703).

La figura 8 describe el proceso de verificación de identidad. El proceso SABA Genérico utilizado para proteger sistemas monitorizados, para recolectar datos, para definir un perfil de usuario, y para alertar al propietario cuando existe una acción no autorizada. Después se instalan los agentes en los sistemas protegidos, el SABA empieza a recibir datos.

Los datos se recolectan mediante el Agente Recuperador de Identidad Teórico (TIRA) (800) y el Agente Recolector de Datos de Autenticación Personal (PADCA) (801).

Cuando un usuario hace una nueva acción sobre un sistema protegido, la TIRA (800) recolecta información que incluye ID, ID de Recursos, Fuente, Aplicación, Versión, etcétera y la envía al almacén de datos TADR (803). Cuando se recibe mediante el sistema esta información no se valida. En este punto, lo llamamos Solicitud de Datos de Autenticación Teórica (TADR) (803). Para calificar estos datos y saber si el solicitante es el propietario, un delegado, o un ladrón, la Autenticación de Fondo Asincrónica Secundaria procederá como sigue:

- Todos los datos obtenidos del TIRA se definen como Solicitud de Datos de Autenticación Teórica (TADR)

- Se utiliza ID de usuario o ID de Recurso (804) para encontrar un perfil de usuario (805) en el almacén de datos PADO (806)

- Luego, el sistema compara los perfiles delegados y de propietario en el Almacén de datos PADO con el perfil del Solicitante en el almacén de datos TADR (807).

▪ Si el resultado de la comparación entre el perfil del solicitante y el perfil del propietario o delegado coincide: (808):

▪ El sistema almacena los datos recolectados del perfil del solicitante para actualizar el perfil del propietario o delegado en el almacén de datos PADO (810).

▪ El sistema actualiza directamente en el almacén (811) de datos PADO el perfil del propietario y delegado con todos los datos rastreados (igual ID e igual fuente) relacionado con la actividad del propietario o delegado y recibido desde el PADCA (801).

▪ Si el resultado de la comparación entre el perfil del solicitante y un perfil del propietario o delegado no coincide: (809):

▪ El sistema envía una alerta al propietario (812)

▪ Si el propietario valida en el sistema que él es el iniciador de la acción el sistema almacena los datos recolectados del perfil del solicitante para actualizar el perfil del propietario en el almacén de datos PADO (810) y actualiza directamente el almacén de datos PADO (811) el perfil del propietario con todos los datos rastreados (igual ID e igual fuente) relacionado con la actividad del propietario y recibido desde el PADCA (801).

▪ Si el propietario está informado de que sus datos han estado comprometidos y pueden tomar todas las acciones necesarias rápidamente (813).

El proceso de Protección de Respaldo, como se describe en la figura 9, se basa en diferentes agentes (900) instalados en los sistemas protegidos. Estos agentes se utilizan para recolectar datos de sistemas de registro (por ejemplo, auditar archivos en Microsoft Windows Server, servidor de archivos Unix, etcétera) (901), software respaldo (por ejemplo, Tivoli, NetBackup, etcétera) (902), o aplicaciones específicas (por ejemplo, aplicación de seguridad para registro de uso de dispositivos de retiro como llaves USB o discos de la empresa) (903) y proteger el lugar en donde los archivos de respaldo se almacenan con un sistema de archivos hecho en casa (904).

El sistema de extrapolación y análisis (AES) (905) agrega todos los datos para definir qué acción se toma sobre un archivo de respaldo y quien lo está haciendo (906).

Se define una lista de personal autorizado y archivos de respaldo, así como la configuración del software de respaldo por el administrador (907) del sistema IT. Dependiendo del software de respaldo utilizado en la compañía, esta lista de puede actualizar o no automáticamente.

Los AES comparan todos los datos recolectados de los agentes con la lista (908) predefinida. Si el resultado identifica a un usuario o acción no autorizada, todo se registra y se envía una alerta a la persona designada (jefe de seguridad por ejemplo (909)) para advertirlo y proporcionarle máxima información. Él puede luego investigar para identificar si existe un ladrón o un problema en su sistema. De otra forma, el sistema conserva la monitorización de los archivos de respaldo (910).

Proceso de protección de fuga de datos:

El proceso de fuga de datos se basa en diferentes agentes (1000) instalados en los sistemas protegidos. Estos agentes se utilizan para recolectar datos de Servidores de Archivos (por ejemplo, Auditoría de Archivos en Microsoft Windows Server, servidor de archivos Unix, etcétera) (1001), Print Server (por ejemplo, Print Server in Microsoft Windows Server, LPD en Linux server, etcétera) (1002), servidores de buzón (por ejemplo, Microsoft Exchange, Postfix, Zimbra, Sendmail, etcétera) (1004) o PBX/IP PBX (por ejemplo, Asterisk, OmniPBX, etcétera) (1003).

Todos los datos recibidos de estos agentes mediante el sistema de análisis y extrapolación (AES) (1005) se utiliza para definir qué archivos se leen, imprimen o envían, quién está haciendo la acción, quién es llamado, y qué tipo de sujetos definen el intercambio de correo (1006).

Un servidor de red segura, basado en AES, deja a una persona designada (CIO de la compañía, por ejemplo) especificar qué es información crítica (por ejemplo: documentos confidenciales, proyectos secretos, planes de reestructuración, etcétera) o competidores o personas quienes pueden tener acceso a esta información. Esto genera una lista de sujetos, contactos y usuarios autorizados (1007).

El AES compara todos los datos recolectados de los agentes con la lista definida (1008). Si el resultado identifica que se imprime un documento confidencial, un intercambio de correo contiene un asunto crítico, se llama a la competencia o se tiene acceso a archivos secretos mediante usuarios no autorizados, se registran los datos y se envía una alerta a una persona designada (por ejemplo, CIO (1009)) para advertirlo y proporcionarle la máxima información. Él puede luego investigar para identificar si existe un ladrón o un problema en su compañía. El sistema continúa monitorizando los intentos de fugas de datos (1010).

Realización 1: Agentes recolectores

De acuerdo con esta realización, los agentes son códigos de software. De acuerdo con una realización preferida, los agentes son programas de software que pueden leer y extraer datos técnicos (registro) generados por hardware, sistemas, o un software instalado en un entorno IT. El equipo de red, servidores, ordenadores, sistemas operativos, sistemas de gestión de bases de datos, sistemas de correo, sitios de red, o software ERP y CRM, son componentes de una infraestructura TI que crea registros. Esta información son datos técnicos relativos a la eficiencia, acciones realizadas o problemas detectados en un sistema.

Existen 3 tipos de agentes recolectores:

i. Monitorizar los sistemas protegidos

II. Recolectar las acciones del propietario y delegados

III. Recolectar la posición del dispositivo del propietario y delegado

El mismo agente puede ser de diferentes tipos y proporcionar toda la información detallada anteriormente.

Los Agentes Recolectores para monitorizar sistemas protegidos:

Aquellos agentes se desarrollan para proporcionar todas las conexiones y todos los intentos para acceder a los sistemas definidos como críticos. Un sistema crítico es un entorno que es monitoriza y protege mediante el sistema SABA. Pueden ser ordenadores, servidores, redes, sistemas de bases de datos o correo, programas o sitios de red. Los agentes reciben todos los registros de conexión y los envían a un módulo de extracción. Luego los datos se transfieren al motor recolector que se va a almacenar y se almacenan y en el Grupo de Datos TADR que se va a procesar mediante los sistemas de análisis y extrapolación que utilizan reglas y algoritmos complejos para determinar si o no se tiene acceso por un usuario autorizado.

Agentes recolectores para recolectar acciones del propietario y delegados:

Estos agentes se desarrollan para proporcionar todas las acciones hechas por el propietario y delegados en un sistema monitorizado. Estos datos se desarrollaron en casa para asegurar que la información se recupera de manera segura de los sistemas y asegurar la identidad del propietario y delegado. Los agentes reciben todos los registros delegados del propietario y los envía a un módulo de extracción. Luego este dato se transfiere a un Motor Recolector que se va a almacenar y se almacena en el Grupo de Datos PADO antes de compararse con los datos TADR mediante los Sistemas de Análisis y Extrapolación.

Agentes recolectores para recolectar posiciones de dispositivos de propietario y delegados:

Estos agentes se desarrollan para proporcionar las posiciones de los dispositivos de propietario y delegados. Estos datos se desarrollan en casa para asegurar que la información se recupera de manera segura a de los dispositivos monitorizados y asegura la identidad del propietario y delegado. Los agentes reciben todas las posiciones del propietario y delegados y las envían a un módulo de extracción. Luego estos datos se transfieren al motor recolector para ser almacenados y se almacenan en el grupo de datos PADO que se compara mediante los Sistemas de Análisis y Extrapolación, con la posición pre calculada de los datos emitidos desde el grupo de datos TADR.

Ejemplo 1

En un sistema de correo Exchange 2010 SP1, el agente recolector es capaz de leer registros de sistemas y obtener más información que aquella proporcionada de naturalmente. Los datos técnicos se recolectan a partir del sistema y se transfieren a un módulo extractor.

Realización 2: Módulo Extractor de datos

Los módulos Extractores de Datos se utilizan para recolectar todos los datos técnicos proporcionados por los agentes recolectores y transferirlos al Motor Recolector en el Administrador Servidor Central (CSM). Estos módulos se pueden instalar en el entorno TI del usuario o sobre el dispositivo del usuario.

Existen 2 tipos de módulos extractores:

a. Módulo Extractor local (LEM)

b. Módulo Extractor de Geolocalización (GEM)

Un módulo extractor puede ser de diferentes tipos dependiendo del lugar en donde se instala.

Módulo Extractor local:

El Módulo Extractor Local se utiliza para recolectar todos los datos técnicos acerca de las acciones y conexiones proporcionadas por el agente recolector en el entorno del usuario TI. Luego los datos recolectados se transfieren al motor recolector en el CSM que se va a procesar. El LEM se puede asociar con un agente recolector en el mismo programa instalado dependiendo de las opciones de usuario y dependiendo del tamaño del entorno IT del usuario.

Módulo Extractor de Geolocalización:

El módulo Extractor de Geolocalización se utiliza para recolectar todos los datos de posición proporcionados por los agentes recolectores instalados en el dispositivo del usuario o la información de eventos relacionados generados por la actividad del usuario. Los datos recolectados se transfieren luego al motor recolector en el CSM que se va a procesar. El GEM se puede asociar con un agente recolector en el mismo programa instalado dependiendo de las opciones del usuario y dependiendo del tamaño del entorno IT del usuario.

Ejemplo 2

En un entorno de TI de usuario, del agente recolector PBX, el sistema puede deducir si el usuario monitoreado está utilizando su teléfono en su oficina; desde el Agente Recolector de Rastreo de Ordenador, el sistema puede saber qué usuario monitorizado está en su oficina utilizando su ordenador y recuperar su posición; del Agente Recolector de Presencia, el sistema obtiene inmediatamente el estado de presencia y también su localización; del agente recolector de calendario, el sistema puede saber su ubicación y agenda; y de los Agentes Recolectores de Pago, el sistema sabe el lugar en donde se hizo la transacción y deduce la posición del usuario monitorizado.

En un IPhone, la aplicación instalada comprende un agente recolector de posición de datos que obtiene geoposición proporcionada por el GPS del teléfono inteligente o triangulación GSM y un GEM transfiere esta información a la Administración de Servidor Central para ser geocodificada y procesada mediante el Sistema de Análisis y Extrapolación.

Realización 3: Motor recolector

El motor recolector es la primera etapa del procesamiento de datos en el Administrador de Servidor Central. Se utiliza para definir la clase de datos recibidos de los módulos extractores. Si los datos corresponden a nuevas conexiones o acciones sobre un sistema protegido, la información se transfiere al Procesador de Flujo de Datos TADR y se almacena en el grupo de datos TADR. Si los datos corresponden a acciones realizadas por un propietario sobre un entorno monitorizado, la información se transfiere al procesador de flujo de datos PADO y se almacena en el grupo de datos PADO. Si los datos corresponden a la posición y Geolocalización del dispositivo de usuario, la información se transfiere al sistema de Geolocalización y se almacena en PADO después de ser geocodificado.

Ejemplo 3

Todos los datos recolectados se envían al Administrador Servidor Central sin ser identificados antes. El Motor Recolector funciona como un interruptor que identifica el tipo de datos y que los transfiere al procesador dedicado.

Realización 4: Sistema de Análisis y Extrapolación

El Sistema de Análisis y Extrapolación (AES) es el núcleo del sistema SABA. El AES es el módulo que almacena, recupera, manipula, ejecuta reglas funcionales y de extrapolación y la comparación con los datos TADR, datos PADO

y datos de Geolocalización para definir si el solicitante es quien dice ser. Cada propietario tiene reglas específicas y perfiles, basados en la información recolectada por el agente recolector y enviada por el extractor o datos llenados directamente por el propietario a través del sitio de red de Gestión y Configuración, y almacenado en el grupo de datos PADO. El Sistema de Análisis y Extrapolación utiliza esta información y la compara con el evento de Solicitud Inicial recibido del flujo de datos TADR para definir si el solicitante es el propietario. Las Reglas son expresiones booleanas divididas en 2 tipos, reglas de Grant o reglas de Deny. Cuando una de las expresiones Grant booleanas resulta que es igual a cero, o cuando una de las Expresiones booleanas Deny es superior a cero, se genera una alerta y se transfiere al Sistema de Alerta.

Ejemplo 4

El Procesador de Datos TADR obtiene información acerca de una nueva conexión del buzón del Director Ejecutivo de la compañía. Esta conexión es una conexión de acceso de red en 1 AM durante días hábiles.

- Las reglas que definen el Director Ejecutivo de la compañía dicen que los usuarios nunca tienen conexión de acceso de red, de tal manera que la expresión booleana de esta regla de Deny es superior a cero (se prohíbe el acceso de red), se genera una alerta.

- Los perfiles almacenados en el grupo de datos PADO del Director Ejecutivo dice que el Director Ejecutivo de la compañía utiliza el acceso de red todas las noches para leer sus mensajes de correo electrónico, de tal manera que la expresión booleana de las reglas de Grant es diferente de cero (por lo menos se define una acción como otorgada), no se genera alerta, el sistema protegido se utiliza normalmente.

Realización 5: Sistema de alertas

El sistema de alertas se utiliza para gestionar todas las alertas. Primero analiza la alerta generada por el Sistema de Análisis y Extrapolación y define si se genera la misma alerta antes. Si existe la misma alerta, busca aproximadamente su estado (abierto, cerrado) y ejecuta la acción asociada. En el caso de una misma alerta abierta, el Sistema de Alertas extiende la alerta existente con una nueva, sin enviar la alerta al propietario. En el caso de una misma alerta cerrado o si no hay alerta, el Sistema de Alerta envía al propietario correcto utilizando el método preferido de alerta (SMS, correo electrónico, llamada, etcétera) y lo etiqueta en un estado de alerta abierto.

Ejemplo 5

Se identifica una nueva conexión de acceso de red desde París sobre un sistema protegido y el Sistema de Análisis y Extrapolación define que esta conexión no se hizo por el propietario, se genera una alerta.

- La misma conexión se identifica dos horas antes, el Sistema de Alertas envía una alerta al propietario y deja la alerta en estado abierto. Ahora el Sistema de Alerta no genera una nueva alerta, extiende la alerta vieja con una nueva.

- Nunca hubo conexión a acceso desde París antes, el Sistema de Alertas envía una alerta al propietario para informarle de una amenaza potencial en su buzón y almacena esta alerta en estado abierto.

Realización combinada: Sistema SABA

Cuando se asocian todas las realizaciones, el Sistema SABA es capaz de recibir datos técnicos desde el entorno del propietario y determina si el último acceso en este sistema protegido fue o no una amenaza. Si la amenaza es real, se envía una alerta al propietario.

REIVINDICACIONES

1. Un sistema para detectar intentos no autorizados para acceder a datos críticos almacenados en un recurso monitorizado y alertar a un propietario o custodio de dicho recurso monitorizado acerca de dichos intentos, el sistema comprende:

un sistema de archivos de respaldo de protección local en comunicación con dicho recurso monitorizado y configurado para controlar el acceso a y el uso de archivos de respaldo críticos para dicho recurso monitorizado;

un sistema recolector local que comprende agentes recolectores configurados para leer datos técnicos de recursos monitorizados y enviar datos técnicos a uno o más módulos extractores de recolección local; dichos módulos extractores de recolección local se configuran para recolectar datos técnicos de agentes y enviar datos a un sistema central;

un sistema recolector de Geolocalización que comprende agentes de Geolocalización instalados en dispositivos de usuario configurados para leer datos de Geolocalización de dispositivos de usuario y enviar datos de Geolocalización a módulos extractores de Geolocalización; dichos módulos extractores de Geolocalización se configuran para recolectar datos de Geolocalización de agentes de Geolocalización y enviar datos a un sistema central;

un módulo de gestión de sistema central en comunicación con el sistema de archivos de respaldo de protección local, los módulos extractores de recolección local y los módulos extractores de Geolocalización, dicho módulo de gestión de sistema central comprende una base de datos de sistema, un sistema de extrapolación y análisis, y un sistema de alerta,

la base de datos del sistema incluye grupos de datos temporales para procesamiento de datos recolectados, datos de autenticación personal para propietarios, PADO, de recursos monitorizados; una solicitud de datos de autenticación teórica (TADR), grupos de datos para todas las nuevas conexiones en recursos monitorizados; y un grupo de datos técnico para reglas y configuraciones;

el sistema de análisis y extrapolación comprende:

un motor recolector configurado para recibir información de sistemas recolectores locales, y agregar y extrapolar datos asociados con la información recibida y un motor de análisis que detecta acceso no autorizado a bases de datos críticas en un procesador de análisis de tipo para identificar el tipo de datos, los procesadores de flujos de datos para construir el perfil, para geocodificar y enviar datos al almacén de datos asociado; y

una Reglas Funcionales y de Extrapolación de procesador; y

el sistema de alertas se configura para comunicarse con el sistema de análisis y extrapolación y enviar mensajes a los propietarios de los recursos monitorizados.

2. El sistema de la reivindicación 1, en el que los Sistemas de Protección Local se instalan en el sistema de respaldo TI del usuario.

3. El sistema de la reivindicación 1, en el que el Sistema de Archivos de Respaldo controla el acceso a archivos de respaldo críticos y evita el acceso a cualquier archivo de respaldo en un sistema no protegido.

4. El sistema de la reivindicación 3, en el que el control de acceso se basa en un tratamiento específico en el archivo de respaldo para protegerlo de ser utilizado en otro sistema.

5. El sistema de la reivindicación 1, en el que los sistemas recolectores locales se instalan en un entorno TI de usuario y se utilizan para recolectar datos técnicos y enviarlos al Administrador de Servidor Central.

6. El sistema de la reivindicación 1, en el que el sistema recolector de Geolocalización se instala en el entorno TI de usuario o en los dispositivos de usuario, y se utilizan para recolectar datos de Geolocalización y enviarlos al Administrador de Servidor Central.

7. El sistema de la reivindicación 1, en el que los agentes recolectores son un grupo de programas que recuperan información de fuentes instaladas en dispositivos de usuario monitorizados, aplicaciones, que incluyen Sistemas Protegidos, y sistemas que son pertinentes.

8. El sistema de la reivindicación 1, en el que la base de datos del sistema incluye Datos de Autenticación Personal de propietario, PADO, grupos de datos que contienen toda la información verificada disponible acerca de un propietario, dicho PADO incluye:

• Usos de usuario hechos de:

- Usos de trabajo,

- Usos de dispositivo,

- Usos de aplicación,

• Geolocalización de usuario definida de la actividad y dispositivos.

9. El sistema de la reivindicación 1, en el que la base de datos del sistema incluye solicitud de datos de autenticación teórica, TADR, grupos de datos que contienen todas las informaciones del solicitante.

10. El sistema de la reivindicación 1, en el que el Motor de Análisis incluye:

a. Un Procesador de Análisis de Tipo

b. Un Procesador de Flujo de Datos TADR

c. Un Procesador de Flujo de Datos PADO

d. Un Sistema de Geolocalización

e. Un Procesador de Reglas Funcionales y de Extrapolación.

11. Un método para detectar un acceso no autorizado a datos críticos, el método comprende las etapas de:

a. Proteger en el entorno TI de usuario, acceso y uso de archivo de respaldo crítico utilizando un Sistema de Archivos de Propietario;

b. Recolectar datos técnicos del entorno TI de usuario;

c. Recolectar datos de Geolocalización de los dispositivos de usuario;

d. Recibir datos técnicos de una nueva conexión o nueva acción en un entorno monitorizado denominado solicitante de datos de autenticación teórico, TADR;

e. Recibir datos técnicos del entorno TI y el dispositivo del propietario que definen el perfil de propietario denominado Datos de Autenticación Personal de Propietario, PADO;

f. Aplicar una o más pruebas basados en diferentes reglas para identificar y validar los datos TADR;

g. Aplicar una o más comparaciones entre el perfil del propietario y el perfil del solicitante para validar que el solicitante es el propietario;

h. Generar alertas;

i. Enviar las alertas a un contacto predefinido cuando se identifica un acceso no autorizado.

12. El método de la reivindicación 11, en el que la protección del archivo de respaldo utiliza un Sistema de Archivo Propietario que utiliza el sistema de archivo ACL, Lista de Control de Acceso, para identificar acciones y acceso de usuarios en archivos de respaldo seguros.

13. El método de la reivindicación 11, en el que la protección del archivo de respaldo utiliza un Sistema de Archivo de Propietario que utiliza un cifrado hecho en casa que evita el uso de archivo de respaldo en otro Sistema de Archivos.

14. El método de la reivindicación 11, en el que los datos recolectados del entorno TI del usuario comprenden formatos de archivos de texto estandarizados de cualquiera de los sistemas de registro que incluyen, pero no se limitan a, fecha, hora, ID de usuario, Dirección IP de Cliente, Aplicación Solicitada, Acción de Usuario, Método de Acceso.

15. El método de la reivindicación 11, en el que los datos recolectados del dispositivo de usuario comprenden un formato de intercambio GPS en un esquema XML que incluye Latitud, Longitud, Altitud, Precisión Horizontal, Precisión Vertical, Velocidad y Datos de Curso.

16. El método de la reivindicación 11, en donde los datos técnicos recibidos por el TADR comprenden un formato XML estandarizado que incluye nueva conexión y nueva acción en entornos protegidos.

17. El método de la reivindicación 11, en el que los datos técnicos recibidos PADO comprenden un formato XML estandarizado que incluye acciones de conexiones estabilizadas en entornos protegidos.

18. El método de la reivindicación 11, en el que las reglas aplicadas en las reivindicaciones 15, 16 y 17 se utilizan para identificar acceso no autorizado a datos críticos.

19. El método de la reivindicación 18, en el que el acceso no autorizado a datos críticos se define mediante un valor Booleano calculado a partir de una pluralidad de reglas predefinidas.

20. El método de la reivindicación 11, en el que las comparaciones aplicadas comprenden un perfil TADR y un tipo de perfil PADO.

21. El método de la reivindicación 20, en el que el tipo de perfil PADO comprende:

A. Usos de trabajo,

B. Usos de dispositivo,

C. Usos de aplicación,

D. Usos de Geolocalización de usuario.

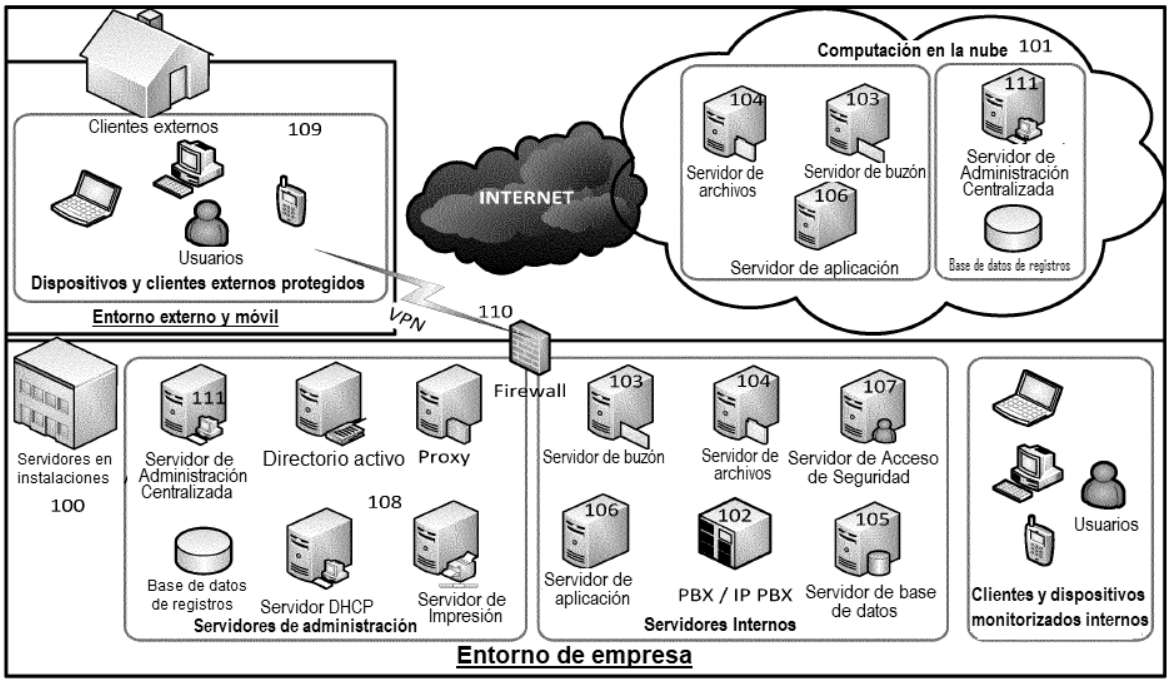
Computación en la nube 101
Clientes externos
109
INTERNET
104
Servidor de archivos
103
Servidor de buzón
106
Servidor de aplicación
111
Servidor de Administración Centralizada
Base de datos de registros
Usuarios
Dispositivos y clientes externos protegidos
Entorno externo y móvil
VPN
110
Firewall
Servidores en instalaciones
100
111
Servidor de Administración Centralizada
Directorio activo
Proxy
108
Base de datos de registros
Servidor DHCP
Servidor de Impresión
Servidores de administración
103
Servidor de buzón
104
Servidor de archivos
107
Servidor de Acceso de Seguridad
106
Servidor de aplicación
102
PBX / IP PBX
105
Servidor de base de datos
Servidores Internos
Usuarios
Clientes y dispositivos monitorizados internos
Entorno de empresa

FIG. 1

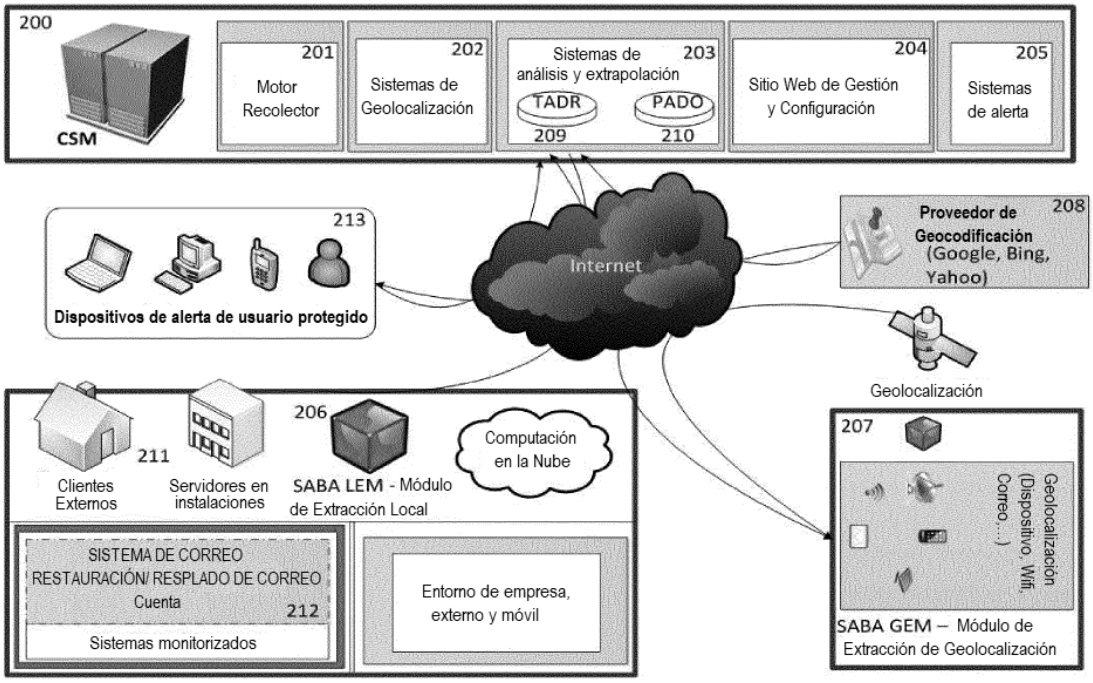
200
CSM
201
Motor Recolector
202
Sistemas de Geolocalización
203
Sistemas de análisis y extrapolación
TADR
209
PADO
210
204
Sitio Web de Gestión y Configuración
205
Sistemas de alerta
213
Dispositivos de alerta de usuario protegido
Internet
208
Proveedor de Geocodificación (Google, Bing, Yahoo)
Geolocalización
206
211
Clientes Externos
Servidores en instalaciones
SABA LEM - Módulo de Extracción Local
Computación en la Nube
SISTEMA DE CORREO
RESTAURACIÓN/ RESPLADO DE CORREO
Cuenta
212
Sistemas monitorizados
Entorno de empresa, externo y móvil
207
Geolocalización (Dispositivo, Wifi, Correo,...)
SABA GEM – Módulo de Extracción de Geolocalización

FIG. 2

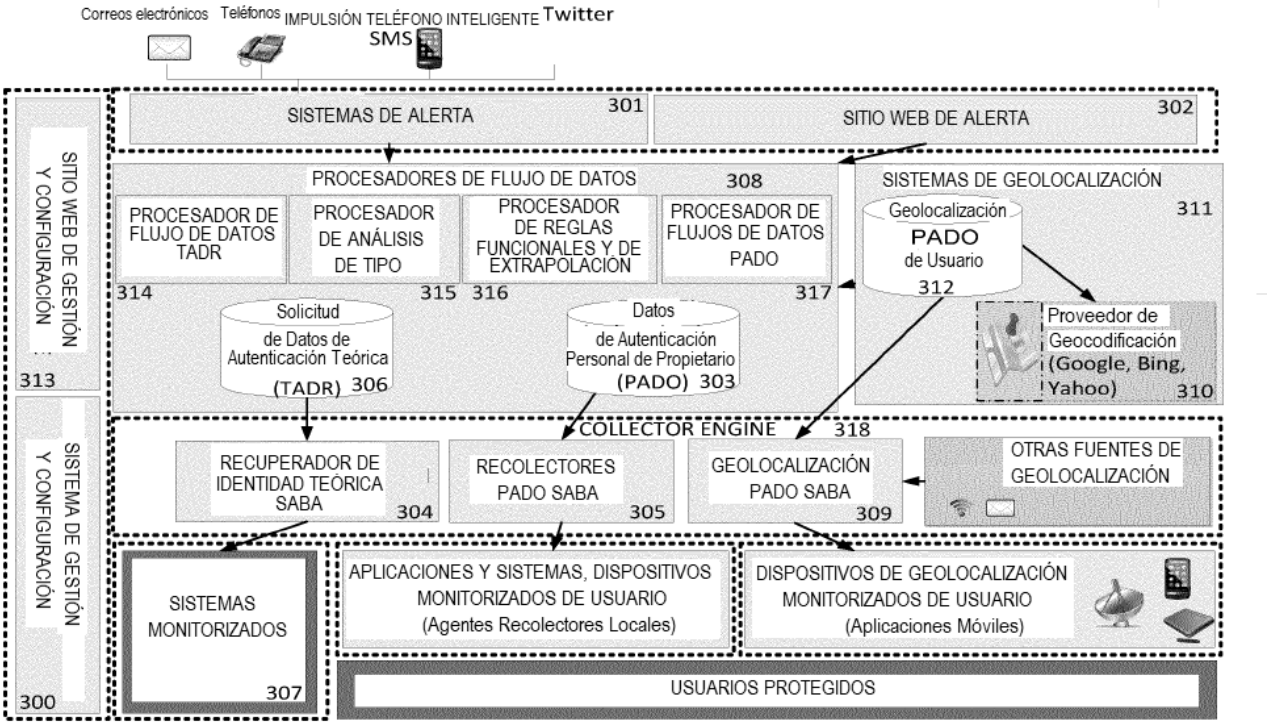
Correos electrónicos
Teléfonos
IMPULSIÓN TELÉFONO INTELIGENTE
SMS
Twitter
SISTEMAS DE ALERTA
301
SITIO WEB DE ALERTA
302
SITIO WEB DE GESTIÓN Y CONFIGURACIÓN
313
PROCESADORES DE FLUJO DE DATOS
308
PROCESADOR DE FLUJO DE DATOS TADR
PROCESADOR DE ANÁLISIS DE TIPO
PROCESADOR DE REGLAS FUNCIONALES Y DE EXTRAPOLACION
PROCESADOR DE FLUJOS DE DATOS PADO
314
315
316
317
SISTEMAS DE GEOLOCALIZACIÓN
311
Geolocalización
PADO
de Usuario
312
Solicitud de Datos de Autenticación Teórica (TADR) 306
Datos de Autenticación Personal de Propietario (PADO) 303
Proveedor de Geocodificación (Google, Bing, Yahoo)
310
SISTEMA DE GESTIÓN Y CONFIGURACIÓN
300
COLLECTOR ENGINE
318
RECUPERADOR DE IDENTIDAD TEÓRICA SABA
304
RECOLECTORES PADO SABA
305
GEOLOCALIZACIÓN PADO SABA
309
OTRAS FUENTES DE GEOLOCALIZACIÓN
SISTEMAS MONITORIZADOS
307
APLICACIONES Y SISTEMAS, DISPOSITIVOS MONITORIZADOS DE USUARIO (Agentes Recolectores Locales)
DISPOSITIVOS DE GEOLOCALIZACIÓN MONITORIZADOS DE USUARIO (Aplicaciones Móviles)
USUARIOS PROTEGIDOS

FIG. 3

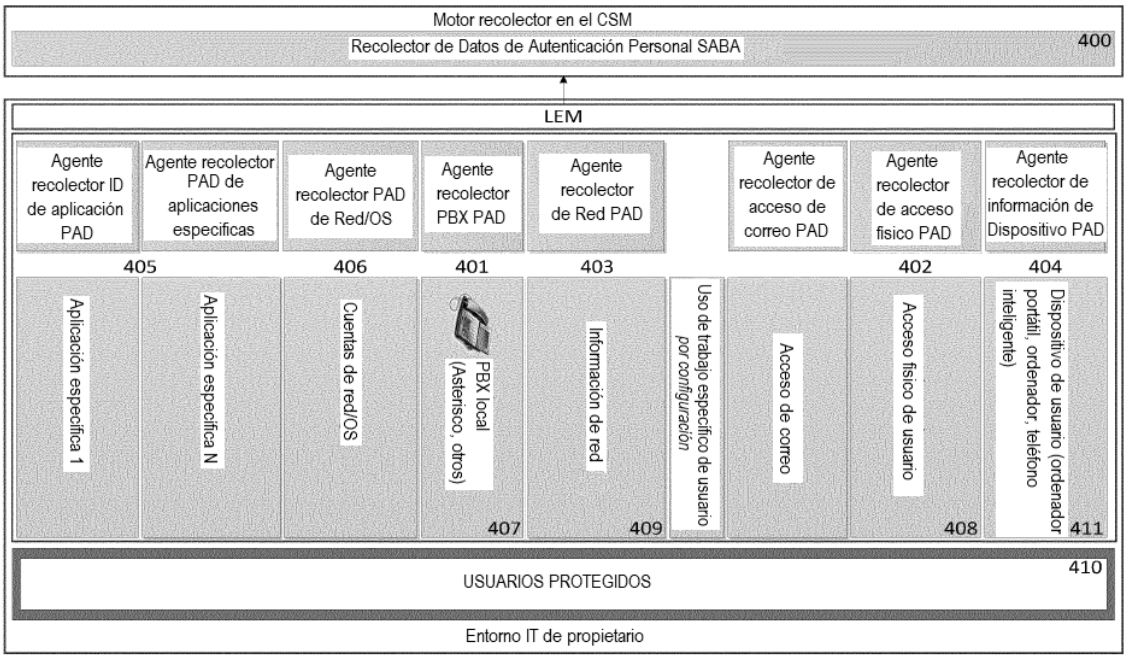
Motor recolector en el CSM
Recolector de Datos de Autenticación Personal SABA
400
LEM
Agente recolector ID de aplicación PAD
Agente recolector PAD de aplicaciones especificas
Agente recolector PAD de Red/OS
Agente recolector PBX PAD
Agente recolector de Red PAD
Agente recolector de acceso de correo PAD
Agente recolector de acceso fisico PAD
Agente recolector de información de Dispositivo PAD
405
406
401
403
402
404
Aplicación especifica 1
Aplicación especifica N
Cuentas de red/OS
PBX local (Asterisco, otros)
Información de red
Uso de trabajo especifico de usuario por configuración
Acceso de correo
Acceso fisico de usuario
Dispositivo de usuario (ordenador portátil, ordenador, teléfono inteligente)
407
409
408
411
USUARIOS PROTEGIDOS
410
Entorno IT de propietario

FIG. 4

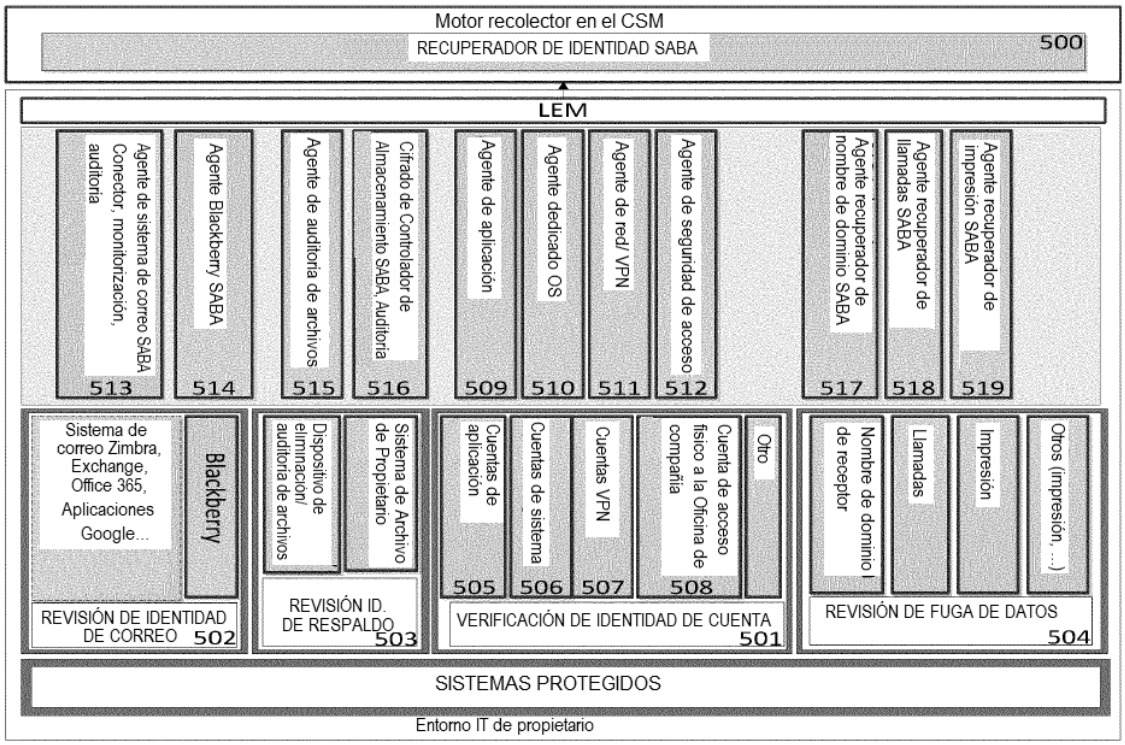
Motor recolector en el CSM
RECUPERADOR DE IDENTIDAD SABA
500
LEM
Agente de sistema de correo SABA Conector, monitorización, auditoría
513
Agente Blackberry SABA
514
Agente de auditoría de archivos
515
Cifrado de Controlador de Almacenamiento SABA, Auditoría
516
Agente de aplicación
509
Agente dedicado OS
510
Agente de red/ VPN
511
Agente de seguridad de acceso
512
Agente recuperador de nombre de dominio SABA
517
Agente recuperador de llamadas SABA
518
Agente recuperador de impresión SABA
519
Sistema de correo Zimbra, Exchange, Office 365, Aplicaciones Google...
Blackberry
REVISIÓN DE IDENTIDAD DE CORREO 502
Dispositivo de eliminación/ auditoría de archivos
Sistema de Archivo de Propietario
REVISIÓN ID. DE RESPALDO 503
Cuentas de aplicación
505
Cuentas de sistema
506
Cuentas VPN
507
Cuenta de acceso físico a la Oficina de compañía
508
Otro
VERIFICACIÓN DE IDENTIDAD DE CUENTA 501
Nombre de dominio de receptor
Llamadas
Impresión
Otros (impresión, ...)
REVISIÓN DE FUGA DE DATOS 504
SISTEMAS PROTEGIDOS
Entorno IT de propietario

FIG. 5

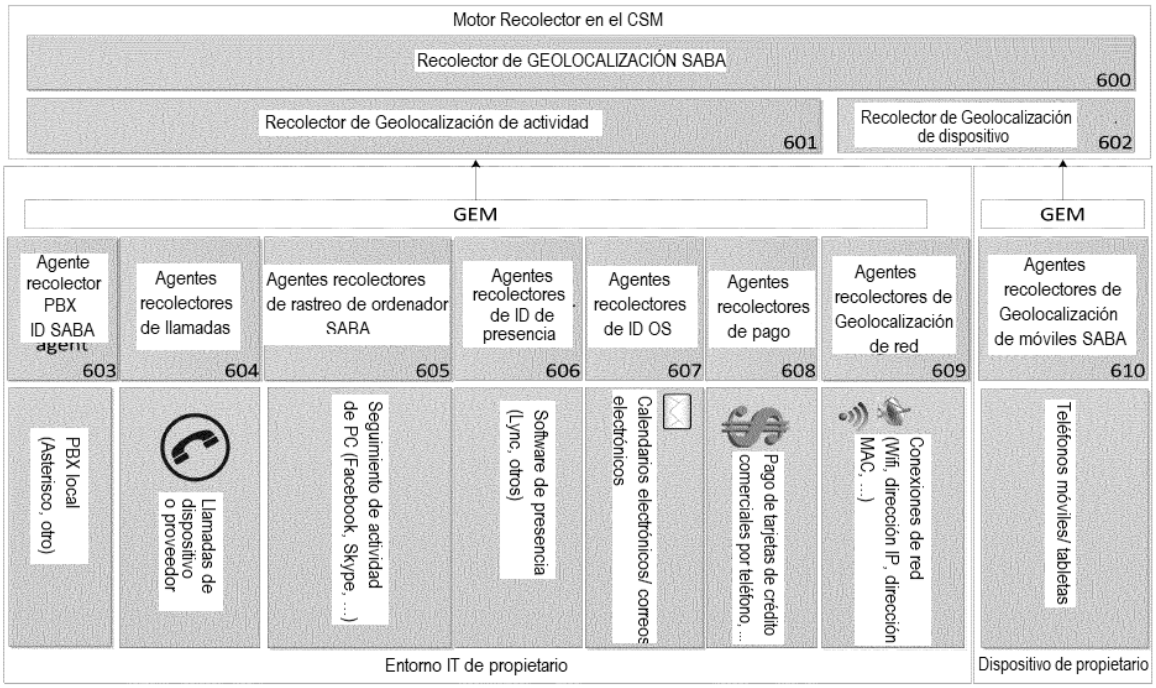
Motor Recolector en el CSM
Recolector de GEOLOCALIZACIÓN SABA
600
Recolector de Geolocalización de actividad
601
Recolector de Geolocalización de dispositivo
602
GEM
GEM
Agente recolector PBX ID SABA
603
Agentes recolectores de llamadas
604
Agentes recolectores de rastreo de ordenador SABA
605
Agentes recolectores de ID de presencia
606
Agentes recolectores de ID OS
607
Agentes recolectores de pago
608
Agentes recolectores de Geolocalización de red
609
Agentes recolectores de Geolocalización de móviles SABA
610
PBX local (Asterisco, otro)
Llamadas de dispositivo o proveedor
Seguimiento de actividad de PC (Facebook, Skype, ...)
Software de presencia (Lync, otros)
Calendarios electrónicos/ correos electrónicos
Pago de tarjetas de crédito comerciales por teléfono, ...
Conexiones de red (Wifi, dirección IP, dirección MAC, ...)
Teléfonos móviles/ tabletas
Entorno IT de propietario
Dispositivo de propietario

FIG. 6

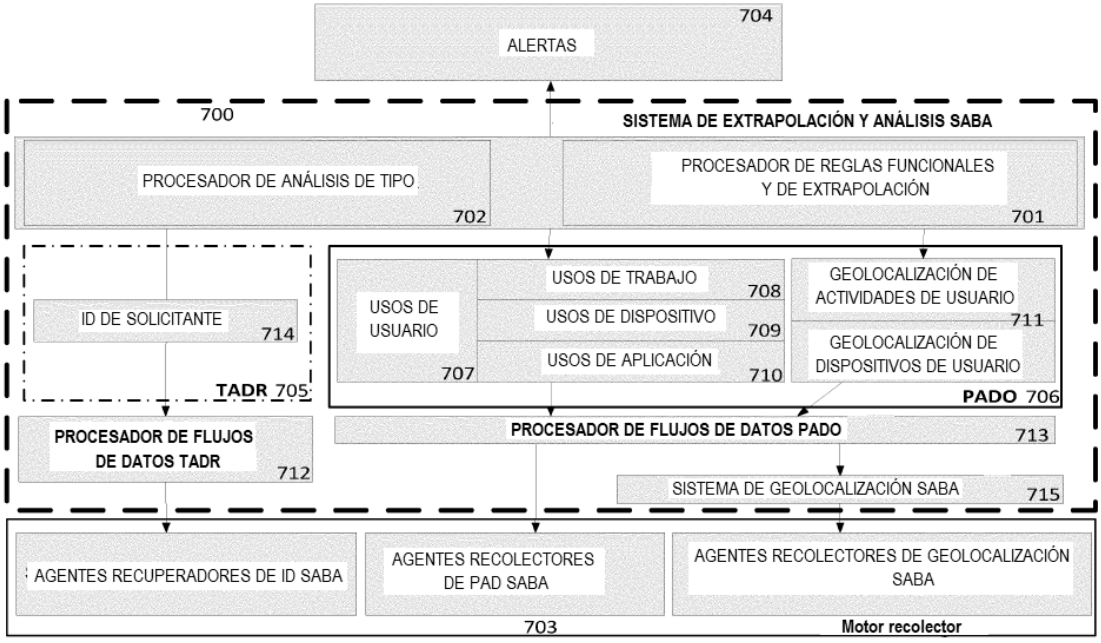
704
ALERTAS
700
SISTEMA DE EXTRAPOLACIÓN Y ANÁLISIS SABA
PROCESADOR DE ANÁLISIS DE TIPO
702
PROCESADOR DE REGLAS FUNCIONALES Y DE EXTRAPOLACIÓN
701
ID DE SOLICITANTE
714
TADR 705
USOS DE USUARIO
707
USOS DE TRABAJO
708
USOS DE DISPOSITIVO
709
USOS DE APLICACIÓN
710
GEOLOCALIZACIÓN DE ACTIVIDADES DE USUARIO
711
GEOLOCALIZACIÓN DE DISPOSITIVOS DE USUARIO
PADO 706
PROCESADOR DE FLUJOS DE DATOS TADR
712
PROCESADOR DE FLUJOS DE DATOS PADO
713
SISTEMA DE GEOLOCALIZACIÓN SABA
715
AGENTES RECUPERADORES DE ID SABA
AGENTES RECOLECTORES DE PAD SABA
703
AGENTES RECOLECTORES DE GEOLOCALIZACIÓN SABA
Motor recolector

FIG. 7

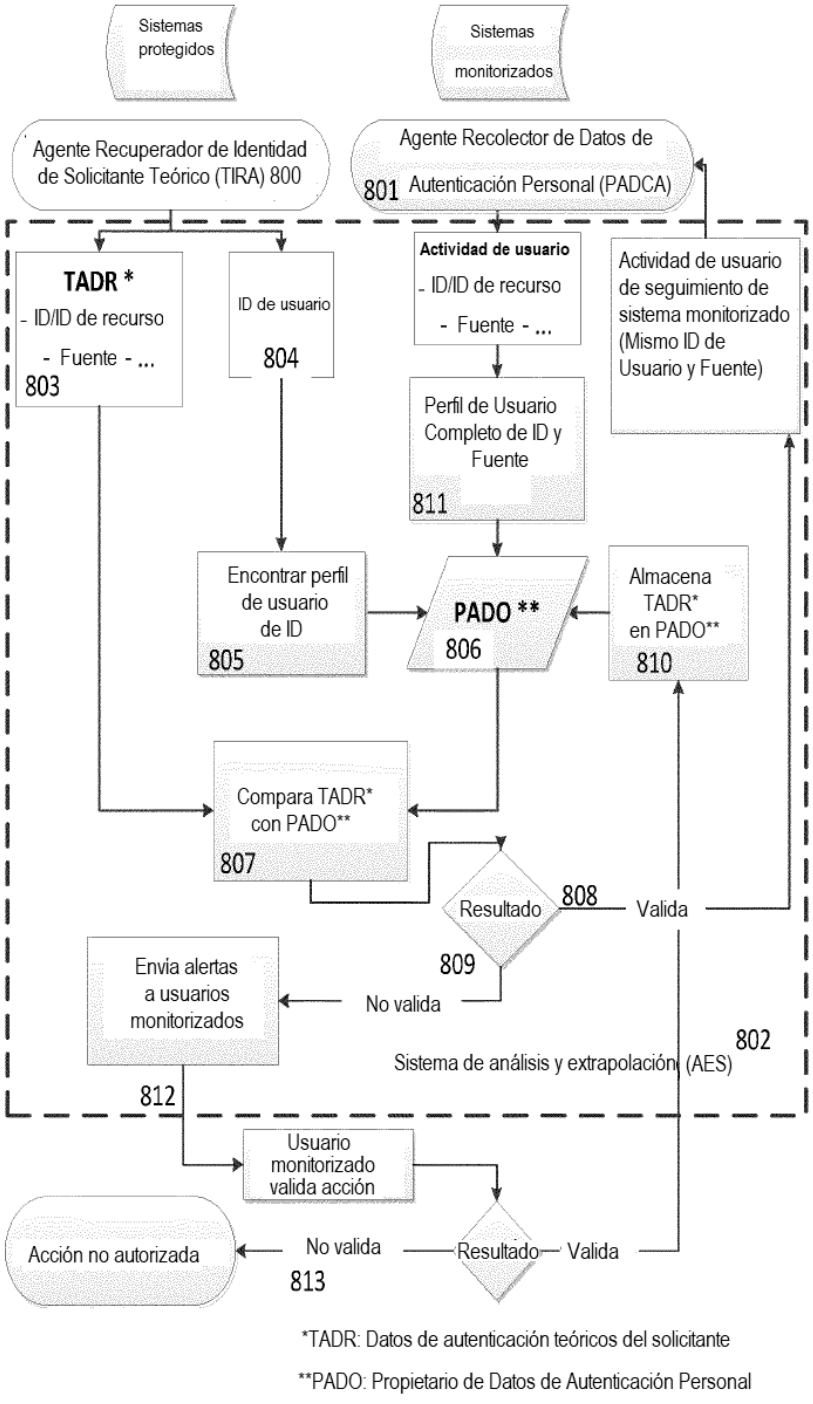
Sistemas protegidos
Sistemas monitorizados
Agente Recuperador de Identidad de Solicitante Teórico (TIRA) 800
Agente Recolector de Datos de Autenticación Personal (PADCA)
801
TADR *
- ID/ID de recurso
- Fuente - ...
803
ID de usuario
804
Actividad de usuario
- ID/ID de recurso
- Fuente - ...
Actividad de usuario de seguimiento de sistema monitorizado (Mismo ID de Usuario y Fuente)
Perfil de Usuario Completo de ID y Fuente
811
Encontrar perfil de usuario de ID
805
PADO **
806
Almacena TADR* en PADO**
810
Compara TADR* con PADO**
807
Resultado
808
Valida
809
No valida
Envía alertas a usuarios monitorizados
802
Sistema de análisis y extrapolación (AES)
812
Usuario monitorizado valida acción
Acción no autorizada
No valida
813
Resultado
Valida
*TADR: Datos de autenticación teóricos del solicitante
**PADO: Propietario de Datos de Autenticación Personal

FIG. 8

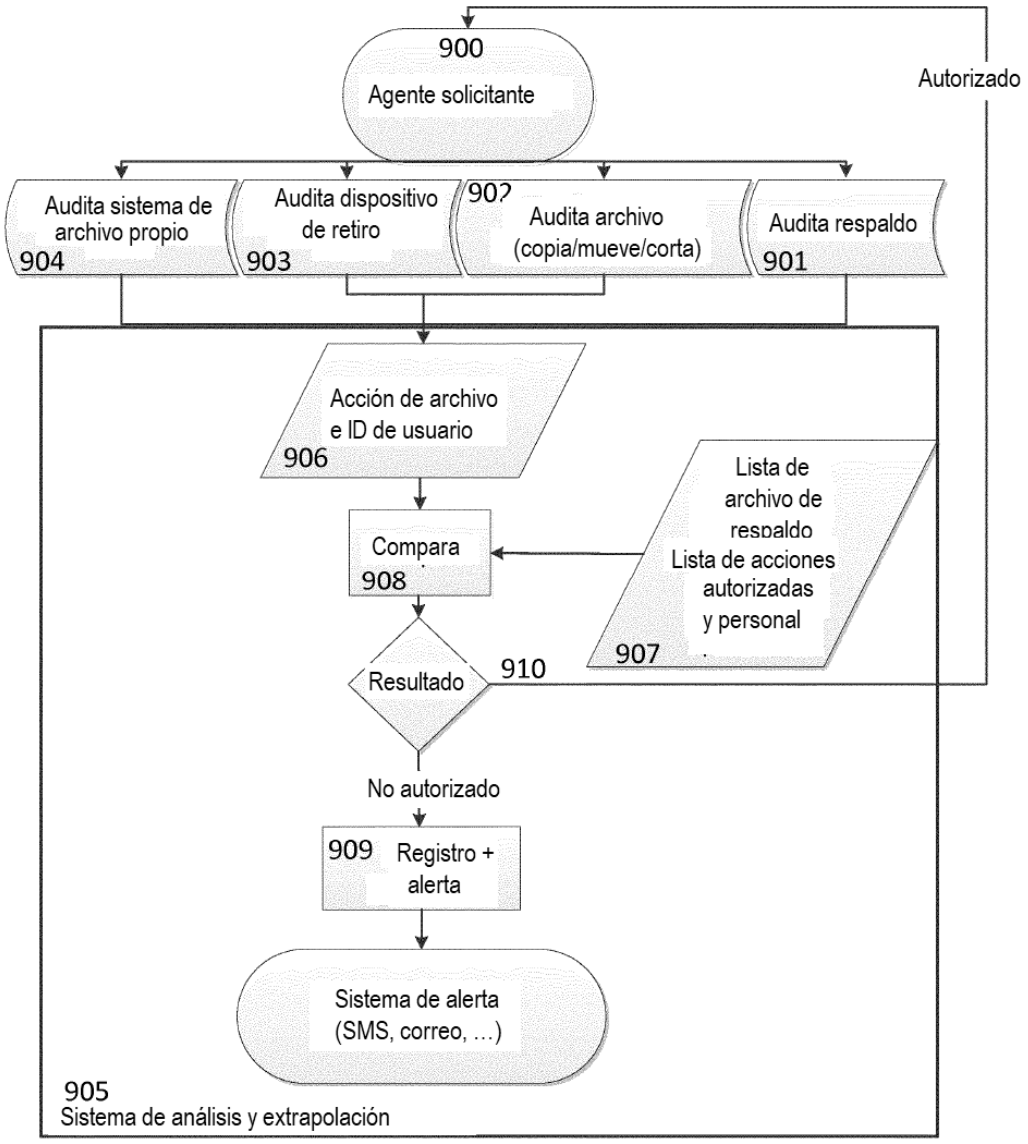
900
Agente solicitante
Autorizado
Audita sistema de archivo propio
904
Audita dispositivo de retiro
903
902
Audita archivo (copia/mueve/corta)
Audita respaldo
901
Acción de archivo e ID de usuario
906
Compara
908
Lista de archivo de respaldo
Lista de acciones autorizadas y personal
907
Resultado
910
No autorizado
909
Registro + alerta
Sistema de alerta (SMS, correo, …)
905
Sistema de análisis y extrapolación

FIG. 9

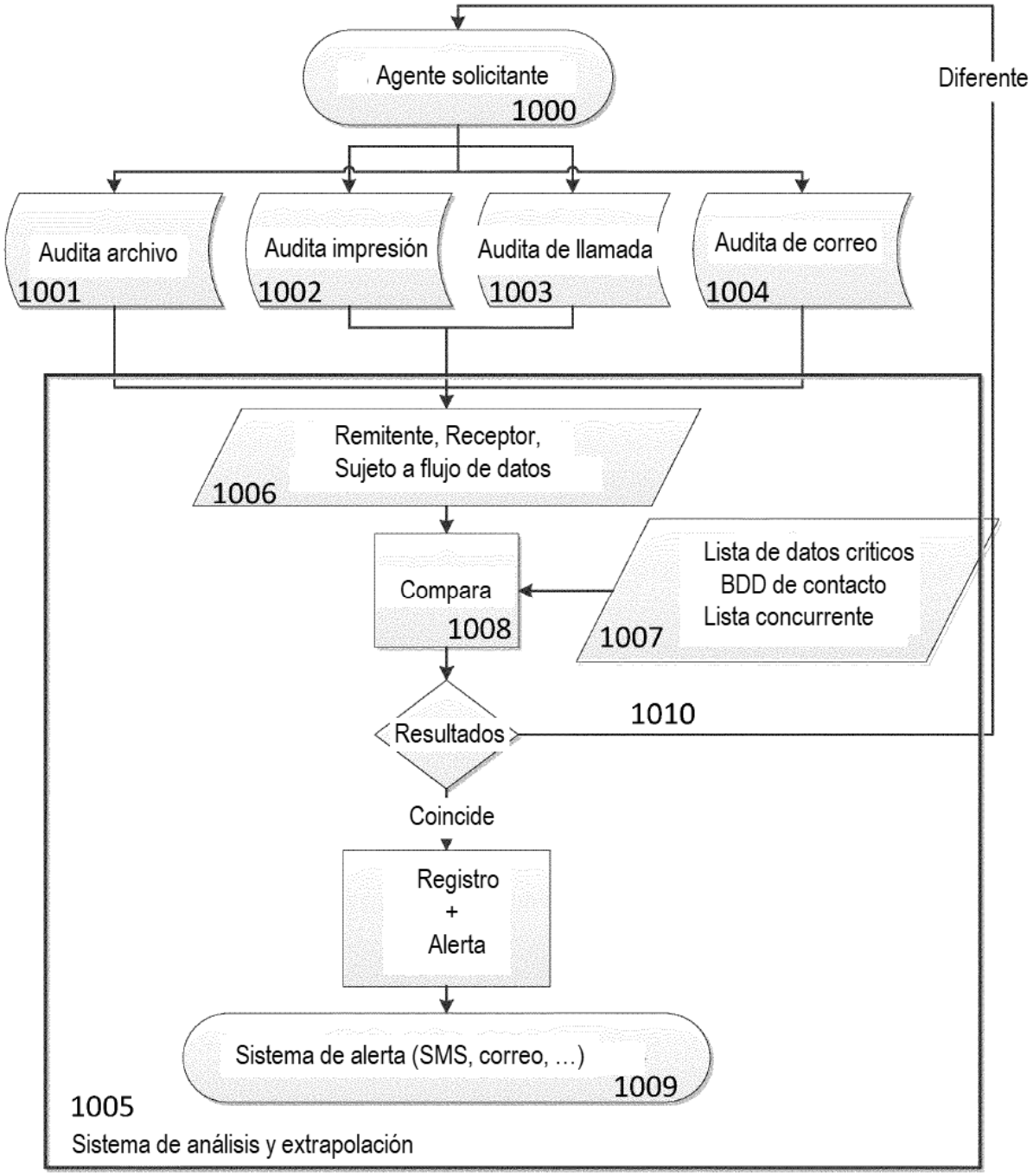
Agente solicitante
1000
Diferente
Audita archivo
1001
Audita impresión
1002
Audita de llamada
1003
Audita de correo
1004
Remitente, Receptor,
Sujeto a flujo de datos
1006
Compara
1008
Lista de datos criticos
BDD de contacto
Lista concurrente
1007
Resultados
1010
Coincide
Registro
+
Alerta
Sistema de alerta (SMS, correo, …)
1009
1005
Sistema de análisis y extrapolación

FIG. 10