(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 767 049**

(51) Int. CI.:

G06F 21/57 (2013.01)
G06F 11/36 (2006.01)
G06F 21/53 (2013.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **19.11.2014 PCT/US2014/066400**

(87) Fecha y número de publicación internacional: **28.05.2015 WO15077331**

(96) Fecha de presentación y número de la solicitud europea: **19.11.2014 E 14810074 (6)**

(97) Fecha y número de publicación de la concesión europea: **30.10.2019 EP 3072079**

(54) Título: **Sistema y método para implementar directivas de aplicación entre entornos de desarrollo**

(30) Prioridad:

19.11.2013 US 201314083750

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
16.06.2020

(73) Titular/es:

VERACODE, INC. (100.0%)
65 Network Drive
Burlington, MA 01803, US

(72) Inventor/es:

CHESTNA, PETER, JOHN

(74) Agente/Representante:

RIZZO , Sergio

DESCRIPCIÓN

Sistema y método para implementar directivas de aplicación entre entornos de desarrollo

Campo de la invención

[0001] La presente invención se refiere en general a la detección y mitigación o eliminación de vulnerabilidades en aplicaciones de *software* y, más en concreto, a sistemas y métodos para llevar a cabo estas operaciones directamente en un binario compilado de una aplicación de *software*.

Antecedentes de la invención

[0002] Las aplicaciones de *software* normalmente son desarrolladas por equipos de programadores, siendo cada uno responsable de funcionalidades o componentes individuales. Para facilitar un desarrollo de aplicaciones rápido, los desarrolladores normalmente programan en paralelo, a menudo en componentes que pueden integrarse con otros elementos de la aplicación. Para apoyar dichas actividades, los entornos de desarrollo convencionales normalmente incluyen un repositorio de código central y entornos de desarrollo individuales separados para cada programador, a los que se les suele denominar «ramas». Los desarrolladores «sacan» código del repositorio central, trabajan en el código en un entorno que está aislado del resto a fin de no introducir errores de programación en la base de código primaria, y una vez que se ha analizado adecuadamente, vuelven a meter el código. Después, un ingeniero de *release* o un ingeniero de control de calidad confirma el nuevo código, compila una nueva instancia de aplicación, y permite que otros accedan al código recién desarrollado para su posterior desarrollo o lanzamiento.

[0003] Por separado, las aplicaciones normalmente se analizan en función de directivas de empresa que regulan el cumplimiento de los criterios de seguridad y vulnerabilidad. No obstante, el uso de directivas a nivel de empresa o de aplicación suele dar como resultado la repetición del trabajo y del esfuerzo, dado que las directivas no se comprueban hasta que se compila la aplicación completa. Por lo general, no existen formas de soportar múltiples flujos de desarrollo de una aplicación independientes y, al mismo tiempo, garantizar que el cumplimiento de las directivas y el análisis a nivel de empresa no se vean afectados de manera adversa. Por tanto, se necesitan técnicas mejoradas para un desarrollo aplicaciones paralelo en varias ramas.

[0004] El documento de patente EP2575069 da a conocer un método para evaluar/analizar vulnerabilidades de *software* durante el proceso de desarrollo, que implica la detección y la solución de vulnerabilidades según las especificaciones de solución y vulnerabilidad almacenadas en la base de datos, que se actualiza una vez que se ha identificado un nuevo tipo de vulnerabilidad.

Sumario de la invención

[0005] La invención se define por las reivindicaciones independientes.

[0006] Varios modos de realización de la presente invención incluyen una plataforma y una metodología que facilita una verificación eficiente del cumplimiento, ya que los desarrolladores trabajan en entornos de desarrollo separados (a los que también se les denomina espacios aislados o ramas). Esto se consigue, al menos en parte, al proporcionar métodos y sistemas de soporte para compartir datos de cumplimiento y directivas centralizadas de vulnerabilidad y seguridad entre los desarrolladores que trabajen en entornos de desarrollo segregados. En concreto, los programadores pueden compartir metadatos, información sobre la mitigación/coincidencia de defectos, y la definición de directivas a través de múltiples análisis independientes y flujos de código. Esto permite que varios desarrolladores analicen la aplicación o una porción de la misma en un entorno segregado en el marco de una única aplicación, pero sin chocar o tener que sincronizarse con un desarrollo de la aplicación paralelo/solapado por otros. No obstante, los desarrolladores pueden recibir cualquier resultado de análisis actualizado en relación con las vulnerabilidades de la aplicación, y pueden analizar el cumplimiento de directivas de sus respectivas ramas en función de dichos resultados actualizados. Por tanto, este entorno general puede evitar o al menos reducir parte de la carga (por ejemplo, la sincronización de una o más ramas), a la vez que explica cualquier impacto que pueda tener este desarrollo en la aplicación completa. Por tanto, pueden encontrarse vulnerabilidades de seguridad en las primeras etapas del ciclo de desarrollo, reduciendo por tanto el coste total de la reparación y evitando que los errores se vuelvan a unir al código base principal. También permite que la gerencia de ingeniería y el equipo de seguridad supervisen al equipo de desarrollo en lo que respecta a las prácticas de programación segura para identificar oportunidades de entrenamiento.

[0007] Por consiguiente, en un aspecto, un método para facilitar un análisis de las vulnerabilidades y una seguridad distribuida de una aplicación de *software* incluye establecer parámetros de directivas de seguridad a nivel de aplicación. El método también incluye distribuir los parámetros de directiva a nivel de aplicación en un espacio aislado de directivas, y distribuir porciones de la aplicación a una serie de espacios aislados de desarrollo. Cada espacio aislado puede estar configurado para permitir un desarrollo adicional de la porción de la aplicación distribuida al mismo. A menudo, el objetivo de dicho desarrollo es reducir el número de vulnerabilidades conocidas y/o proporcionar funcionalidades adicionales. El método incluye además analizar, en uno o más espacios aislados, la parte correspondiente de la aplicación de conformidad con los parámetros de la directiva de seguridad a nivel de aplicación mediante el acceso al espacio aislado de directivas, y actualizar el

espacio aislado de directivas con resultados de análisis de al menos uno de varios espacios aislados de desarrollo.

[0008] Estos resultados actualizados pueden utilizarse en el respectivo análisis en uno o más del resto de espacios aislados. De manera similar, el espacio aislado que se ha de analizar también puede utilizar resultados de análisis actualizados (a los que también se les llama promovidos) del resto de espacios aislados, sin tener que sincronizarse con el resto de espacios aislados, es decir, sin tener que incorporar ningún cambio a la aplicación que se haya hecho en algunos otros espacios aislados al espacio aislado que está siendo analizado. De manera ventajosa, esto puede disminuir sustancialmente el esfuerzo y el tiempo de análisis y/o de desarrollo, dado que la integración rama/espacio aislado y el análisis de la aplicación completa puede llevar mucho tiempo.

[0009] En algunos modos de realización, el método incluye además designar un ID de análisis a los resultados del análisis de la aplicación. Puede calcularse un resultado del cumplimiento con base, al menos en parte, en los resultados del análisis de la aplicación, y el ID de análisis puede asociarse con el resultado del cumplimiento. Los resultados de análisis, el resultado de cumplimiento o ambos pueden almacenarse en el espacio aislado de directivas, por ejemplo, para que los utilicen otros espacios aislados. Los resultados del análisis de la aplicación pueden obtenerse, al menos en parte, al analizar la aplicación de *software* completa utilizando los parámetros de directiva de seguridad a nivel de aplicación. De manera alternativa o adicional, los resultados de análisis de la aplicación pueden incluir resultados de análisis del espacio aislado que se promovieron desde uno o más espacios aislados de desarrollo.

[0010] En algunos modos de realización, cada uno de los varios espacios aislados de desarrollo se corresponde con un ID de análisis. Uno de los espacios aislados es designado como un primer espacio aislado, y el primer espacio aislado se corresponde con una primera porción designada de la aplicación. En estos modos de realización, el análisis de la primera porción de la aplicación incluye: (a) obtener resultados de análisis del primer espacio aislado al analizar, en una primera iteración, la primera porción de la aplicación. También pueden analizarse otras porciones de la aplicación. El análisis también incluye (b) calcular una primera diferencia entre los resultados de análisis del primer espacio aislado y los resultados de análisis de la aplicación asociados con el ID de análisis. Posteriormente, se puede obtener una primera evaluación en el paso (c) al evaluar las restricciones de defectos de directivas con base, al menos en parte, en la primera diferencia.

[0011] En el paso (d), si la primera evaluación falla, la primera porción de la aplicación puede modificarse y volverse a analizar en una segunda iteración, para obtener segundos resultados de análisis de espacio aislado para el primer espacio aislado. Se calcula una segunda diferencia entre los resultados de análisis del segundo espacio aislado y los resultados de análisis de la aplicación asociados con el ID de análisis y/o los resultados de análisis del primer espacio aislado, y puede obtenerse una segunda evaluación al evaluar las restricciones de defectos de directivas con base, al menos en parte, en la segunda diferencia. En estos modos de realización, la actualización del espacio aislado de directivas incluye (e) promover, en el espacio aislado, resultados de análisis promovidos que incluyen los resultados de análisis del primer espacio aislado si la primera evaluación se completa correctamente, o los resultados de análisis del segundo espacio aislado si la segunda evaluación se completa correctamente.

[0012] En varios modos de realización, se incluye un segundo espacio aislado dentro de los varios espacios aislados de desarrollo, y el segundo espacio aislado se corresponde con una segunda porción designada de la aplicación. El análisis de la porción correspondiente (es decir, la segunda porción) de la aplicación incluye además llevar a cabo los pasos (a) a (d) con respecto al segundo entorno aislado. Además, la actualización del espacio aislado de directivas incluye además llevar a cabo el paso (e) con respecto al segundo espacio aislado. El análisis de las primeras y segundas porciones de la aplicación en los primeros y segundos espacios aislados, respectivamente, pueden solaparse al menos en parte con el tiempo.

[0013] Los parámetros de la directiva de seguridad a nivel de aplicación pueden incluir parámetros de frecuencia de análisis, parámetros de restricción de defectos, o ambos. Los parámetros de frecuencia de análisis pueden incluir uno o varios de entre: (i) un tipo de análisis, comprendiendo el tipo de análisis al menos uno de entre análisis estático, dinámico, manual y de comportamiento, y (ii) una frecuencia de análisis, comprendiendo la frecuencia al menos uno de entre una vez, mensual, trimestral y anual. Las restricciones de defectos pueden incluir uno o varios de entre la enumeración de debilidades comunes (CWE, del inglés *Common Weakness Enumeration*), la categoría del defecto, la gravedad del defecto y una restricción estandarizada con base, al menos en parte, en al menos uno de entre el proyecto abierto de seguridad de aplicaciones web (OWASP, del inglés *Open Web Application Security Project*), el Instituto SANS (del inglés *SysAdmin Audit, Networking and Security Institute*), un equipo de respuesta ante emergencias informáticas (CERT, del inglés *Computer Emergency Response Team*) y el estándar para la Industria de Tarjeta de Pago (PCI, del inglés *Payment Card Industry*).

[0014] En otro aspecto, un sistema para facilitar un análisis de vulnerabilidad y seguridad distribuida de una aplicación de *software* incluye una memoria que incluye al menos una porción de los parámetros de la directiva de seguridad a nivel de aplicación, y un primer procesador acoplado a la memoria. El primer procesador está configurado para proporcionar un primer espacio aislado de desarrollo que está adaptado para recibir una

primera porción de la aplicación completa. El primer espacio aislado también está adaptado para calcular y/o recibir los resultados de análisis de la aplicación. El primer espacio aislado de desarrollo puede permitir un desarrollo adicional de la primera porción de la aplicación recibida en el mismo. De manera adicional, el primer procesador está configurado para evaluar la primera porción de la aplicación de conformidad con al menos una porción de los parámetros de la directiva de seguridad a nivel de aplicación, a fin de obtener resultados de análisis del primer espacio aislado, y para actualizar un espacio aislado de directivas con los resultados de análisis del primer espacio aislado

[0015] En algunos modos de realización, a fin de evaluar la primera porción de la aplicación, el primer procesador está configurado para: (a) obtener resultados iniciales del análisis del espacio aislado al analizar en una primera iteración la primera porción de la aplicación, (b) calcular una diferencia inicial entre los resultados del análisis del espacio aislado y los resultados del análisis de la aplicación, y (c) obtener una evaluación inicial al evaluar restricciones de defectos de directiva con base, al menos en parte, en la diferencia inicial. El primer procesador está configurado de manera adicional para: (d) si la evaluación falla, (A) obtener resultados de análisis del espacio aislado al analizar en una segunda iteración la primera porción de la aplicación, y (B) calcular una diferencia revisada entre los resultados del análisis del espacio aislado revisados y uno o más de los resultados del análisis de la aplicación, los resultados del análisis de espacio aislado inicial, y cualquier resultado del análisis del espacio aislado revisado previamente. Antes de volver a analizar en la segunda iteración, puede modificarse la primera porción de la aplicación, por ejemplo, para solucionar determinadas vulnerabilidades de seguridad conocidas. El primer procesador también está configurado (C) para obtener una evaluación revisada al evaluar las restricciones de defectos de directivas con base, al menos en parte, en la diferencia revisada. Asimismo, para actualizar el espacio aislado de la directiva, el primer procesador está configurado además para: (e) designar como resultados de análisis del primer espacio aislado los resultados de análisis de espacio aislado iniciales si la evaluación inicial se completa con éxito, o los resultados de análisis de espacio aislado revisados si la evaluación revisada se completa con éxito, y (f) promover, en el espacio aislado de directivas, los resultados de análisis del primer espacio aislado.

[0016] En algunos modos de realización, el sistema incluye de manera adicional un segundo procesador acoplado a la memoria. El segundo procesador está configurado para proporcionar un segundo espacio aislado de desarrollo adaptado para recibir una segunda porción de la aplicación completa. El segundo espacio aislado, que puede permitir un desarrollo adicional de la segunda porción de la aplicación recibida en el mismo, también está adaptado para calcular y/o recibir los resultados de análisis de la aplicación. El segundo procesador está configurado además para evaluar la segunda porción de la aplicación de conformidad con al menos una porción de los parámetros de la directiva de seguridad a nivel de aplicación, a fin de obtener segundos resultados de análisis de espacio aislado. Además, el segundo procesador está adaptado para actualizar el espacio aislado de directivas con los resultados de análisis del segundo espacio aislado.

[0017] En algunos modos de realización, los primeros y segundos procesadores son diferentes, mientras que en otros modos de realización, un procesador único representa a los primeros y segundos procesadores. El primer espacio aislado de desarrollo normalmente es distinto al segundo espacio aislado de desarrollo. Los resultados de análisis de la aplicación pueden incluir resultados de análisis de la aplicación iniciales, resultados de análisis de la aplicación actualizados en el espacio aislado de directivas, o ambos. Los resultados de análisis de la aplicación actualizados en el espacio aislado de directivas puede promoverse en el mismo desde uno o más de los espacios aislados, p. ej., el primer espacio aislado de desarrollo, un segundo espacio aislado de desarrollo, etc.

[0018] En algunos modos de realización, el sistema incluye además un servidor configurado para proporcionar el espacio aislado de directivas y para calcular los resultados de análisis de la aplicación iniciales con base, al menos en parte, en el análisis de la aplicación de *software* completa. El primer procesador puede adaptarse para recibir los resultados de análisis de la aplicación. El servidor puede estar configurado para designar los resultados de análisis de la aplicación actualizados como los resultados de análisis de la aplicación iniciales. El servidor puede configurarse de manera adicional para designar un ID de análisis a los resultados de análisis de la aplicación iniciales, y para calcular y asociar con el ID de análisis, un resultado de cumplimiento con base, al menos en parte, en los resultados de análisis de la aplicación iniciales. Asimismo, el servidor puede estar configurado para almacenar los resultados de cumplimiento asociados con el ID de análisis en el espacio aislado de directivas.

[0019] En algunos modos de realización, el servidor está configurado para designar un ID de análisis a los resultados de análisis de aplicación iniciales, y para calcular y asociar al ID de análisis, un resultado de cumplimiento con base, al menos en parte, en los resultados de análisis de aplicación actualizados. El servidor puede estar configurado además para almacenar los resultados de cumplimiento asociados con el ID de análisis en el espacio aislado de directivas. Un único procesador puede estar configurado a la vez como primer procesador y servidor.

[0020] En otro aspecto, un artículo manufacturado que incluye un medio legible por máquina no transitorio que almacena instrucciones que, cuando son ejecutadas por una máquina que comprende una memoria y un procesador en comunicación electrónica con la memoria, configuran la memoria para almacenar al menos una

porción de los parámetros de directiva de seguridad a nivel de aplicación. Asimismo, para facilitar una seguridad distribuida y un análisis de las vulnerabilidades de una aplicación de *software*, las instrucciones configuran el procesador para que proporcione un primer espacio aislado de desarrollo que está adaptado para recibir una primera porción de la aplicación completa. El primer espacio aislado también está adaptado para calcular y/o recibir resultados de análisis de la aplicación. El primer espacio aislado de desarrollo puede permitir un desarrollo adicional de la primera porción de la aplicación recibida en el mismo. Según las instrucciones, el primer procesador está configurado además para analizar la primera porción de la aplicación con arreglo a al menos una porción de los parámetros de directiva de seguridad a nivel de aplicación, a fin de obtener resultados de análisis del primer espacio aislado, y para actualizar un espacio aislado de directivas con los primeros resultados de análisis de espacio aislado.

[0021] En algunos modos de realización, a fin de evaluar la primera porción de la aplicación, las instrucciones configuran el primer procesador para: (a) obtener resultados de análisis del espacio aislado iniciales al analizar en una primera iteración la primera porción de la aplicación, (b) calcular una diferencia inicial entre los resultados de análisis del espacio aislado y los resultados de análisis de la aplicación, y (c) obtener una evaluación inicial al evaluar restricciones de defectos de directivas con base, al menos en parte, en la diferencia inicial. Las instrucciones configuran de manera adicional el primer procesador para: (d) si la evaluación falla, (A) obtener resultados de análisis de espacio aislado revisados al analizar en una segunda iteración la primera porción de la aplicación, y (B) calcular una diferencia revisada entre los resultados de análisis de espacio aislado revisados y uno o más de los resultados de análisis de aplicación, los resultados de análisis de espacio aislado iniciales, y cualquier resultado de análisis de espacio aislado revisado previamente. Antes de volverse a analizar en la segunda iteración, puede modificarse la primera porción de la aplicación, por ejemplo, para solucionar determinadas vulnerabilidades de seguridad conocidas. Las instrucciones también pueden configurar el primer procesador (C) para obtener una evaluación revisada al evaluar restricciones de defectos de directivas con base, al menos en parte, en la diferencia revisada. Asimismo, para actualizar el espacio aislado de directivas, las instrucciones configuran además el primer procesador para: (e) designar como resultados de análisis del primer espacio aislado los resultados de análisis del espacio aislado iniciales si la evaluación inicial se completa con éxito, o los resultados de análisis del espacio aislado revisados si la evaluación revisada se completa con éxito, y (f) promover, en el espacio aislado de la directiva, los resultados de análisis del primer espacio aislado.

Breve descripción de los dibujos

[0022] Diversos modos de realización de la presente invención descritos en el presente documento se ilustran a modo de ejemplo, y no a modo de limitación, en las figuras de los dibujos adjuntos, en las que:

La figura 1 representa de manera esquemática un sistema de espacio aislado de directivas y el entorno operativo de este, según un modo de realización.

Descripción detallada de la invención

[0023] Haciendo referencia a la figura 1, se generan los metadatos 104 y módulos 106 correspondientes a una aplicación de *software* 102, por ejemplo, por el equipo de desarrollo o el ingeniero de compilación. Una directiva de cumplimiento de vulnerabilidad/seguridad 108 se determina normalmente en el paso 152 mediante una combinación de requisitos de cumplimiento normativo y procedimientos recomendados junto con la importancia crítica comercial de la aplicación. La directiva de cumplimiento puede incluir parámetros como requisitos de frecuencia de análisis 110, restricciones de defectos 112, etc. En general, la frecuencia de análisis dicta el tipo de análisis que se ha de completar (estático, dinámico, manual, de comportamiento, etc.) y con qué frecuencia debe realizarse este análisis (una vez, mensual, trimestral, anual, etc.). Las restricciones de defectos pueden estar configuradas por ítems tales como la enumeración de debilidades comunes individuales (CWE, del inglés *Common Weakness Enumeration*), la categoría del defecto, la gravedad del defecto, o por estándares comunes como OWASP, SANS, CERT y PCI. Una vez que se ha determinado la directiva, en el paso 154 puede asignarse a la aplicación de *software* 102 de manera que pueda asegurarse que posteriores modificaciones de la aplicación de *software* cumplen con la directiva de vulnerabilidad/seguridad 108.

[0024] En este sentido, en varios modos de realización, la directiva se pone a disposición de un espacio aislado de directiva 114. En los pasos 156, 158, la aplicación de *software* a nivel de empresa completa 102 puede analizarse, es decir, examinarse, en un análisis a nivel de aplicación/empresa (p. ej., análisis A1). Los resultados del análisis a nivel de aplicación 116 (p. ej., AT1) del examen pueden cargarse en el espacio aislado de directivas 114. Durante un desarrollo adicional de la aplicación de *software,* el cumplimiento de la directiva puede evaluarse en función de estos resultados y se obtiene un resultado de cumplimiento. En general, los resultados del examen incluyen los defectos detectados durante el análisis, incluyendo cualquier defecto nuevo que se encuentre, defectos descubiertos previamente que sigan abiertos o que se hayan vuelto a abrir, es decir, designados como no solucionados, y defectos encontrados previamente que ya no se encuentran, p. ej., se ha determinado que se han arreglado. Con respecto al espacio aislado de directivas 114, la directiva completa se evalúa en el paso 160, es decir, se detectan y analizan defectos, si los exámenes requeridos por la directiva se llevan a cabo a la frecuencia especificada determinada, y/o tras un periodo de gracia permitido para solucionar defectos. En función de esta evaluación, se determina un estado de cumplimiento de directiva o un valor de

cumplimiento de aplicación 118, p. ej., Conforme, No Conforme, Condicionalmente Conforme, y se actualiza el estado de la directiva en el paso 162. El cumplimiento condicional normalmente tiene en cuenta un periodo de gracia para solucionar nuevos defectos, así como análisis requeridos que aún no se han realizado. En general, los análisis de espacio aislado solo evalúan las reglas basadas en defectos.

[0025] Tras el análisis a nivel de aplicación A1, si la aplicación se ha de modificar y/o analizar bajo distintas condiciones, se crea un espacio aislado 120_0 en el paso 164_0. También pueden crearse espacios aislados adicionales hasta el espacio aislado 120_N. Normalmente, solo una porción del código/programa de aplicación se asigna a cada espacio aislado, aunque el programa de aplicación completo puede asignarse a uno o más espacios aislados. Las porciones asignadas a dos espacios aislados pueden ser idénticas, solaparse parcialmente, o ser distintas. Cada espacio aislado 120_k puede incluir los metadatos 122_k asociados con la aplicación completa o con la porción específica asignada al espacio aislado. Por ejemplo, los metadatos 122_0 están asociados con el espacio aislado 120_0. Normalmente, distintos desarrolladores/programadores pueden, de manera independiente, modificar y/o analizar la porción del programa asignada a cada espacio aislado, respectivamente.

[0026] En un modo de realización, tras modificar una porción asignada a un espacio aislado concreto 120_0 (p. ej., el espacio aislado A1S1), el desarrollador puede evaluar/examinar el espacio aislado en una primera iteración (p. ej., A1S1_1) en los pasos 166a y 168a. La solicitud de análisis crea normalmente una estructura para comenzar el proceso de análisis, para contener resultados de análisis y para evaluar la directiva. En algunos modos de realización, cada solicitud de análisis contiene los metadatos sobre el análisis (p. ej., la fecha en la que se solicitó el análisis, el usuario que lo solicita, el tipo de análisis solicitado, etc.), los archivos que se cargaron y se seleccionaron para el análisis, la configuración de análisis, si la hubiera, cualquier resultado de ese análisis, y la evaluación de directiva de estos resultados.

[0027] Según este análisis/examen, una porción del programa puede dejarse sin cambiar desde el análisis a nivel de empresa anterior A1, pero puede haberse modificado otra porción del programa. Los resultados (p. ej., A1S1T1) de esta iteración de análisis se comparan con los resultados del análisis a nivel de aplicación AT1, y se calcula una diferencia entre estos 124a (p. ej., A1S1D1). La diferencia puede incluir un conjunto de nuevas vulnerabilidades, vulnerabilidades que se han vuelto a abrir o que se han revertido, vulnerabilidades que siguen presentes desde el análisis anterior (es decir, vulnerabilidades abiertas), y vulnerabilidades de un análisis previo que ya no se han encontrado (es decir, vulnerabilidades solucionadas). Después, la directiva de cumplimiento de vulnerabilidades/seguridad se vuelve a evaluar en el paso 170a utilizando los resultados de análisis A1S1T1 y/o la diferencia calculada A1S1D1, tal como se ha descrito anteriormente. En algunos modos de realización, la revaluación en función de la diferencia entre los resultados puede ser más rápida que revaluar la directiva utilizando los resultados completos del análisis.

[0028] En varios modos de realización, volver a evaluar la directiva puede proporcionar un resultado de aprobado/suspenso en el paso 172a en función de los defectos encontrados durante el análisis. Si los defectos detectados previamente se han solucionado y no se han introducido nuevos defectos prohibidos, una iteración puede designarse como aprobada o completada con éxito. En algunos modos de realización, no todos los defectos detectados previamente pueden solucionarse y/o pueden introducirse nuevas vulnerabilidades. No obstante, la iteración puede designarse como aprobada si no hay ningún aumento o disminución del total de defectos sin solucionar que infringen las restricciones de defecto. En el ejemplo anterior, el análisis en la primera iteración puede designarse como suspenso en el paso 172a.

[0029] Si la primera iteración A1S1_1 del análisis del espacio aislado A1S1 falla, el desarrollador puede modificar de manera adicional la porción del programa/código asignada al espacio aislado 120_0 (es decir, A1S1), y puede volver a analizar el espacio aislado en una segunda iteración 166b y 166b (p. ej., A1S1_2), produciendo los resultados A1S1T2. La comparación, el cálculo de la diferencia 124b, y la revaluación en 170b, tal como se ha descrito anteriormente, se repiten, y se obtiene otro resultado de aprobado/suspenso en el paso 172b. Dichas iteraciones para el espacio aislado A1S1 pueden continuar hasta que el esfuerzo de desarrollo consiga requisitos de calidad y funcionales y se consiga un resultado de aprobado. Si el resultado de la iª iteración (i = 1, 2, 3, ..., etc.) es aprobado, los resultados correspondientes A1S1Ti para el espacio aislado A1S1 pueden promoverse al espacio aislado de directiva, p. ej., tras la segunda iteración en el paso 178_0. Hasta que se promueva, otros espacios aislados pueden utilizar estos resultados en sus respectivas evaluaciones.

[0030] Tal como se ha descrito anteriormente, normalmente, distintos programadores/desarrolladores modifican y/o examinan, de manera dependiente, la porción de programa asignada a cada espacio aislado. Por tanto, en un modo de realización, se crea un segundo espacio aislado (p. ej., el espacio aislado A1S2) después del análisis a nivel de aplicación A1. El espacio aislado A1S2 se analiza de manera similar al espacio aislado A1S1, en una o más iteraciones. En una primera iteración, el análisis de este espacio aislado puede producir los resultados de análisis A1S2T1 y una diferencia A1S2D1, tal como se ha descrito anteriormente. Si esta iteración falla, una segunda iteración puede producir los resultados de análisis A1S2T2 y una diferencia A1S2D2. Del mismo modo que sucede con el espacio aislado A1S1, si el resultado de la jª iteración (j = 1, 2, 3, ..., etc.) es un aprobado, los resultados correspondientes A1S2Tj para el espacio aislado A1S2 pueden promoverse al espacio aislado de directivas, y puede compartirse con otros espacios aislados. Las iteraciones y/o promoción del espacio aislado

A1S2 pueden llevarse a cabo de manera sustancialmente paralela con las iteraciones y/o promoción del espacio aislado A1S1, o estas operaciones pueden solaparse en el tiempo solo parcialmente. No obstante, en algunos modos de realización, estas operaciones se llevan a cabo de manera secuencial. Debería entenderse que la exposición de dos iteraciones y dos espacios aislados se hace solo a título ilustrativo, y que varios modos de realización pueden incluir uno o más (p. ej., 5, 10, 12, etc.) espacios aislados y/o iteraciones. Normalmente, aunque no necesariamente, el número de espacios aislados (p. ej., N) es distinto al número de iteraciones para un espacio aislado (p. ej., n). El número de iteraciones máximas y/o realizadas realmente en distintos espacios aislados pueden ser iguales o diferentes.

[0031] Después de analizar varios espacios aislados tal como se ha descrito anteriormente, puede realizarse un segundo análisis a nivel de aplicación/empresa (p. ej., análisis A2) en el paso 180. En el análisis A2, los resultados promovidos de cada uno de los espacios aislados 120_0 a 120_N pueden utilizarse para obtener un conjunto nuevo o actualizado de resultados de análisis a nivel de aplicación 126 (p. ej., AT2). Los resultados de análisis a nivel de aplicación AT1 y AT2 pueden compararse para calcular una diferencia 128 entre ellos. En función de esta diferencia, la directiva puede volverse a evaluar en el paso 182 para obtener resultados de cumplimiento actualizados 130, y el estado de la directiva puede actualizarse en función de los resultados de cumplimiento en el paso 184. Después, puede crearse un nuevo conjunto de espacios aislados, p. ej., A2S1, A2S2, etc., y estos espacios aislados pueden analizarse tal como se ha descrito anteriormente. En algunos modos de realización, no se crean nuevos espacios aislados después del análisis A2, y en su lugar, los espacios aislados creados previamente tras el análisis A1, p. ej., A1S1, A1S2, se reutilizan para realizar nuevos análisis/exámenes, generando nuevos resultados de análisis, y realizando nuevas evaluaciones, de manera similar a la descrita anteriormente.

[0032] Resulta evidente que existen muchas formas de configurar el dispositivo y/o los componentes, interfaces, enlaces de comunicación y métodos del sistema descritos en el presente documento. Los métodos, dispositivos y sistemas dados a conocer se pueden implementar en plataformas de procesador convenientes, entre las que se incluyen servidores de red, ordenadores personales y portátiles y/u otras plataformas de procesamiento. Se pueden contemplar otras plataformas a medida que mejoran las capacidades de procesamiento, incluyendo asistentes personales digitales, relojes informatizados, teléfonos móviles y/u otros dispositivos portátiles. Los métodos y sistemas dados a conocer se pueden integrar en sistemas y métodos de gestión de redes conocidos. Los métodos y los sistemas dados a conocer pueden operar como agente SNMP y pueden configurarse con la dirección IP de una máquina remota que ejecute una plataforma de gestión conforme. Por lo tanto, el alcance de los métodos y los sistemas dados a conocer no está limitado por los ejemplos proporcionados en el presente documento, sino que puede incluir el alcance completo de las reivindicaciones.

[0033] Los métodos, dispositivos y sistemas descritos en el presente documento no están limitados a una configuración de *software* o *hardware* concreta, y pueden encontrar aplicabilidad en muchos espacios informáticos o de procesamiento. Los métodos, dispositivos y sistemas se pueden implementar en *hardware* o *software*, o en una combinación de *hardware* y *software*. Los métodos, dispositivos y sistemas se pueden implementar en uno o más programas informáticos, en los que puede entenderse que un programa informático incluye una o más instrucciones ejecutables por procesador. El programa o los programas informático(s) se puede(n) ejecutar en uno o más elementos o máquinas de procesamiento programables, y se pueden almacenar en uno o más medios de almacenamiento legibles por el procesador (entre los que se incluyen elementos de almacenamiento y/o memoria volátil y no volátil), o uno o más dispositivos de entrada, y/o uno o más dispositivos de salida. Por tanto, los elementos/máquinas de procesamiento pueden acceder a uno o más dispositivos de entrada para obtener datos de entrada, y pueden acceder a uno o más dispositivos de salida para comunicar datos de salida. Los dispositivos de entrada y/o salida pueden incluir uno o más de entre los siguientes: memoria de acceso aleatorio (RAM), matriz redundante de discos independientes (RAID), unidad de disquete, CD, DVD, disco magnético, disco duro interno, disco duro externo, memoria extraíble, u otro dispositivo de almacenamiento al que pueda acceder un elemento de procesamiento según se proporciona en el presente documento, donde dichos ejemplos anteriormente mencionados no son exhaustivos, y se proporcionan a modo de ilustración y no de limitación.

[0034] El programa o programas informático(s) se puede(n) implementar utilizando uno o más lenguajes de programación de alto nivel procedimentales u orientados a objetos para comunicarse con un sistema informático; sin embargo, el programa o programas se pueden implementar en lenguaje ensamblador o de máquina, si se desea. El lenguaje puede compilarse o interpretarse.

[0035] Como se ha proporcionado en el presente documento, el procesador o los procesadores y/o los elementos de procesamiento pueden estar integrados, por tanto, en uno o más dispositivos que pueden operarse de forma independiente o conjunta en un entorno de red, donde la red puede incluir, por ejemplo, una red de área local (LAN), una red de área extensa (WAN), y/o puede incluir una intranet y/o el Internet y/u otra red. La(s) red(es) puede(n) ser con cable o inalámbrica(s) o una combinación de estas y puede utilizar uno o más protocolos de comunicaciones para facilitar las comunicaciones entre los diferentes procesadores/elementos de procesamiento. Los procesadores pueden configurarse para un procesamiento distribuido y pueden utilizar, en algunos modos de realización, un modelo de cliente-servidor, según sea necesario. Por consiguiente, los

métodos, dispositivos y sistemas pueden utilizar múltiples procesadores y/o dispositivos de procesador, y las instrucciones del procesador/elemento de procesamiento pueden dividirse entre dicho único o múltiples procesadores/dispositivos/elementos de procesamiento.

[0036] El dispositivo o los dispositivos o los sistemas informáticos que se integran en el/los procesador(es)/elemento(s) de procesamiento pueden incluir, por ejemplo, un ordenador personal o varios, una estación de trabajo (p. ej., Dell, HP), un asistente personal digital (PDA), un dispositivo portátil tal como un teléfono móvil, un ordenador portátil, un dispositivo de mano u otro dispositivo que pueda integrarse en uno o varios procesadores que puedan operar como se proporciona en el presente documento. Por consiguiente, los dispositivos proporcionados en el presente documento no son exhaustivos y se proporcionan para fines de ilustración y no de limitación.

[0037] Se puede entender que las referencias a «un procesador», o «un elemento de procesamiento», «el procesador» y «el elemento de procesamiento» incluyen uno o más microprocesadores que pueden comunicarse en uno o varios espacios independientes y/o distribuidos, y pueden por tanto configurarse para comunicarse mediante comunicaciones con cable o inalámbricas con otros procesadores, donde dichos uno o más procesadores pueden configurarse para operar en uno o más dispositivos controlados por procesador/elementos de procesamiento que pueden ser dispositivos similares o diferentes. Por tanto, también puede entenderse que el uso de la terminología de «microprocesador», «procesador» o «elemento de procesamiento» incluye una unidad de procesamiento central, una unidad lógica aritmética, un circuito integrado (IC) de aplicación específica, y/o un motor de tareas, estando estos ejemplos proporcionados a modo de ilustración y no de limitación.

[0038] Además, las referencias a la memoria, a menos que se especifique lo contrario, pueden incluir uno o más elementos y/o componentes de memoria accesibles y legibles por procesador que pueden ser internos al dispositivo controlado por procesador, externos al dispositivo controlado por procesador, y/o se puede acceder a ellos mediante una red con cable o inalámbrica utilizando varios protocolos de comunicaciones y, a menos que se especifique lo contrario, pueden disponerse para que incluyan una combinación de dispositivos de memoria externos e internos, donde dicha memoria puede ser contigua y/o con particiones en función de la aplicación. Por ejemplo, la memoria puede ser una unidad flash, un disco, CD/DVD, memoria distribuida, etc. Las referencias a las estructuras incluyen enlaces, colas, gráficos, árboles, y estas estructuras se proporcionan a modo de ilustración y no de limitación. Se puede entender que las referencias en el presente documento a instrucciones o instrucciones ejecutables, de conformidad con lo anterior, incluyen *hardware* programable.

[0039] Aunque los métodos y sistemas se han descrito en relación con modos de realización específicos de los mismos, no están limitados a estos. Como tal, pueden resultar evidentes muchas modificaciones y variaciones teniendo en cuenta la información dada a conocer anteriormente. Los expertos en la materia pueden realizar muchos cambios adicionales en los detalles, los materiales y la disposición de partes descritos e ilustrados en el presente documento. Por consiguiente, se entenderá que los métodos, los dispositivos y los sistemas proporcionados en el presente documento no han de limitarse a los modos de realización dados a conocer en el presente documento, pueden incluir prácticas distintas a las descritas específicamente, y han de interpretarse de la forma más amplia que permita la ley.

REIVINDICACIONES

1. Método para facilitar un análisis distribuido de la seguridad y de la vulnerabilidad de una aplicación de *software*, comprendiendo el método:

establecer parámetros de directiva de seguridad a nivel de aplicación;
distribuir los parámetros de la directiva a nivel de aplicación a un espacio aislado de directiva;
distribuir porciones de la aplicación a una pluralidad de espacios aislados de desarrollo, estando cada espacio aislado configurado para permitir un desarrollo adicional de la porción de la aplicación distribuida al mismo,
donde la pluralidad de espacios aislados de desarrollo:

(i) se corresponde con un ID de análisis; y
(ii) comprende un primer espacio aislado de desarrollo, correspondiéndose el primer espacio aislado de desarrollo con una primera porción de la aplicación;

analizar, en al menos un espacio aislado de desarrollo la porción correspondiente de la aplicación, de conformidad con los parámetros de directiva de seguridad a nivel de aplicación mediante un acceso al espacio aislado de directiva,
donde el análisis de la primera porción de la aplicación comprende:

(a) obtener primeros resultados de análisis del espacio aislado de desarrollo al analizar en una primera iteración al menos la primera porción de la aplicación;
(b) calcular una primera diferencia entre los primeros resultados del análisis de espacio aislado de desarrollo y los resultados de análisis de la aplicación que están asociados al ID de análisis;
(c) obtener una primera evaluación al evaluar las restricciones de defecto de directiva con base, al menos en parte, en la primera diferencia;
(d) si la evaluación falla:

(A) obtener segundos resultados de análisis de espacio aislado de desarrollo para el primer espacio aislado de desarrollo al analizar en una segunda iteración la primera porción de la aplicación;
(B) calcular una segunda diferencia entre los segundos resultados de análisis de espacio aislado de desarrollo y al menos uno entre los resultados de análisis de la aplicación asociados al ID de análisis y los primeros resultados de análisis del espacio aislado de desarrollo; y
(C) obtener una segunda evaluación al evaluar las restricciones de defecto de directiva con base, al menos en parte, en la segunda diferencia;

actualizar el espacio aislado de directivas con los resultados de análisis de al menos uno de la pluralidad de espacios aislados de desarrollo;
donde actualizar comprende:
(e) promover, en el espacio aislado de directivas, los primeros resultados de análisis del espacio aislado de desarrollo si la primera evaluación se completa con éxito, o los segundos resultados de análisis de espacio aislado de desarrollo si la segunda evaluación se completa con éxito.

2. Método según la reivindicación 1, comprendiendo además:

designar un ID de análisis para los resultados de análisis de la aplicación;
calcular y asociar al ID de análisis un resultado de cumplimiento con base, al menos en parte, en los resultados de análisis de la aplicación; y
almacenar al menos uno de entre: (i) los resultados de análisis de aplicación que están asociados al ID de análisis, y (ii) el resultado de cumplimiento asociado al ID de análisis, en el espacio aislado de directivas.

3. Método según la reivindicación 2, comprendiendo además analizar la aplicación de *software* completa utilizando los parámetros de directiva de seguridad a nivel de aplicación para obtener los resultados de análisis de aplicación.

4. Método según la reivindicación 2, donde los resultados de análisis de la aplicación comprenden resultados de análisis del espacio aislado promovidos desde al menos un espacio aislado de desarrollo dentro de la pluralidad de espacios aislados.

5. Método según la reivindicación 1, donde la pluralidad de espacios aislados de desarrollo comprende un segundo espacio aislado de desarrollo, correspondiéndose el segundo espacio asilado de desarrollo con una segunda porción de la aplicación;
analizar la porción correspondiente de la aplicación comprende llevar a cabo los pasos (a) a (d) con respecto al segundo espacio aislado de desarrollo; y
actualizar comprende además llevar a cabo el paso (e) con respecto al segundo espacio aislado de desarrollo.

6. Método según la reivindicación 5, donde analizar la primera porción de la aplicación en el primer espacio aislado de desarrollo y analizar la segunda porción de la aplicación en el segundo espacio aislado de desarrollo se solapan al menos parcialmente en el tiempo.

7. Método según la reivindicación 1, donde los parámetros de directiva de seguridad a nivel de aplicación comprenden al menos uno de entre parámetros de frecuencia de análisis y parámetros de restricción de defectos.

8. Método según la reivindicación 7, donde los parámetros de frecuencia de análisis comprenden al menos uno de entre:

(i) un tipo de análisis, comprendiendo el tipo de análisis al menos uno de entre análisis estático, dinámico, manual y de comportamiento, y
(ii) una frecuencia de análisis, comprendiendo la frecuencia al menos uno de entre una vez, mensual, trimestral y anual.

9. Método según la reivindicación 7, donde las restricciones de defecto comprenden al menos uno de entre una enumeración de debilidades comunes individuales (CWE), la categoría del defecto, la gravedad del defecto, y una restricción estandarizada basada, al menos en parte, en al menos uno de los estándares OWASP, SANS, CERT y PCI.

10. Sistema para facilitar el análisis distribuido de la seguridad y de la vulnerabilidad de una aplicación de *software*, comprendiendo el sistema:

una memoria que comprende al menos una porción de parámetros de directiva de seguridad a nivel de aplicación; y
un primer procesador acoplado a la memoria y que está configurado para:

proporcionar un primer espacio aislado de desarrollo adaptado para:

(i) recibir una primera porción de la aplicación completa, y
(ii) al menos uno de entre calcular y recibir resultados de análisis de aplicación, permitiendo el primer espacio aislado de desarrollo un desarrollo adicional de la primera porción de la aplicación recibida en el mismo;

analizar la primera porción de la aplicación de conformidad con al menos una porción de los parámetros de directiva de seguridad a nivel de aplicación, a fin de obtener primeros resultados de análisis del espacio aislado de desarrollo,
donde, para analizar la primera porción de la aplicación, el primer procesador está configurado para:

(a) obtener resultados de análisis del espacio aislado de desarrollo iniciales al analizar en una primera iteración la primera porción de la aplicación;
(b) calcular una diferencia inicial entre los resultados de análisis del espacio aislado de desarrollo iniciales y los resultados de análisis de la aplicación;
(c) obtener una evaluación inicial al evaluar restricciones de defectos de directiva con base, al menos en parte, en la diferencia inicial;
(d) si la evaluación falla:

(A) obtener resultados de análisis del espacio aislado de desarrollo revisados al analizar en una segunda iteración la primera porción de la aplicación;
(B) calcular una diferencia revisada entre los resultados de análisis del espacio aislado de desarrollo revisados y al menos uno de los resultados de análisis de aplicación, los resultados de análisis del espacio aislado de desarrollo iniciales; y
(C) obtener una evaluación revisada al evaluar las restricciones de defecto de directiva con base, al menos en parte, en la diferencia revisada;

actualizar un espacio aislado de directiva con los primeros resultados de análisis del espacio aislado de desarrollo,
donde, para actualizar el espacio aislado de directivas, el primer procesador está configurado además para:

(e) designar como primeros resultados de análisis del espacio aislado de desarrollo a los resultados de análisis del espacio aislado de desarrollo iniciales si la evaluación inicial se completa con éxito, o a los resultados de análisis del espacio aislado de desarrollo revisados si la evaluación revisada se completa con éxito; y
(f) promover, al espacio aislado de directiva, los primeros resultados de análisis del espacio aislado de desarrollo.

11. Sistema según la reivindicación 10, comprendiendo además:

un segundo procesador acoplado a la memoria y que está configurado para:

proporcionar un segundo espacio aislado de desarrollo adaptado para:

(i) recibir una segunda porción de la aplicación completa, y
(ii) al menos uno de entre calcular y recibir los resultados de análisis de la aplicación, permitiendo el segundo espacio aislado de desarrollo un desarrollo adicional de la segunda porción de la aplicación recibida en el mismo;

analizar la segunda porción de la aplicación de conformidad con al menos una porción de los parámetros de directiva de seguridad a nivel de aplicación, a fin de obtener segundos resultados de análisis del espacio aislado de desarrollo; y
actualizar el espacio aislado de directivas con los segundos resultados de análisis de espacio aislado de desarrollo,

12. Sistema según la reivindicación 11, donde los primeros y segundos procesadores son diferentes.

13. Sistema según la reivindicación 11, donde un único procesador comprende el primer procesador y el segundo procesador, y el primer espacio aislado de desarrollo es distinto al segundo espacio aislado de desarrollo.

14. Sistema según la reivindicación 10, donde los resultados de análisis de la aplicación comprenden al menos uno de entre:

(i) resultados de análisis de la aplicación iniciales, y
(ii) resultados de análisis de la aplicación actualizados en el espacio aislado de directivas, promovidos en el mismo desde al menos uno de entre el primer espacio aislado de desarrollo y un segundo espacio aislado de desarrollo.

15. Sistema según la reivindicación 14, comprendiendo además un servidor configurado para proporcionar el espacio aislado de directivas y para calcular los resultados de análisis de la aplicación iniciales con base, al menos en parte, en el análisis de la aplicación de *software* completa, y donde el primer procesador está adaptado para recibir los resultados de análisis de la aplicación.

16. Sistema según la reivindicación 15, donde el servidor está configurado para designar a los resultados de análisis de la aplicación actualizados como los resultados de análisis de la aplicación iniciales.

17. Sistema según la reivindicación 15, donde el servidor está configurado además para:

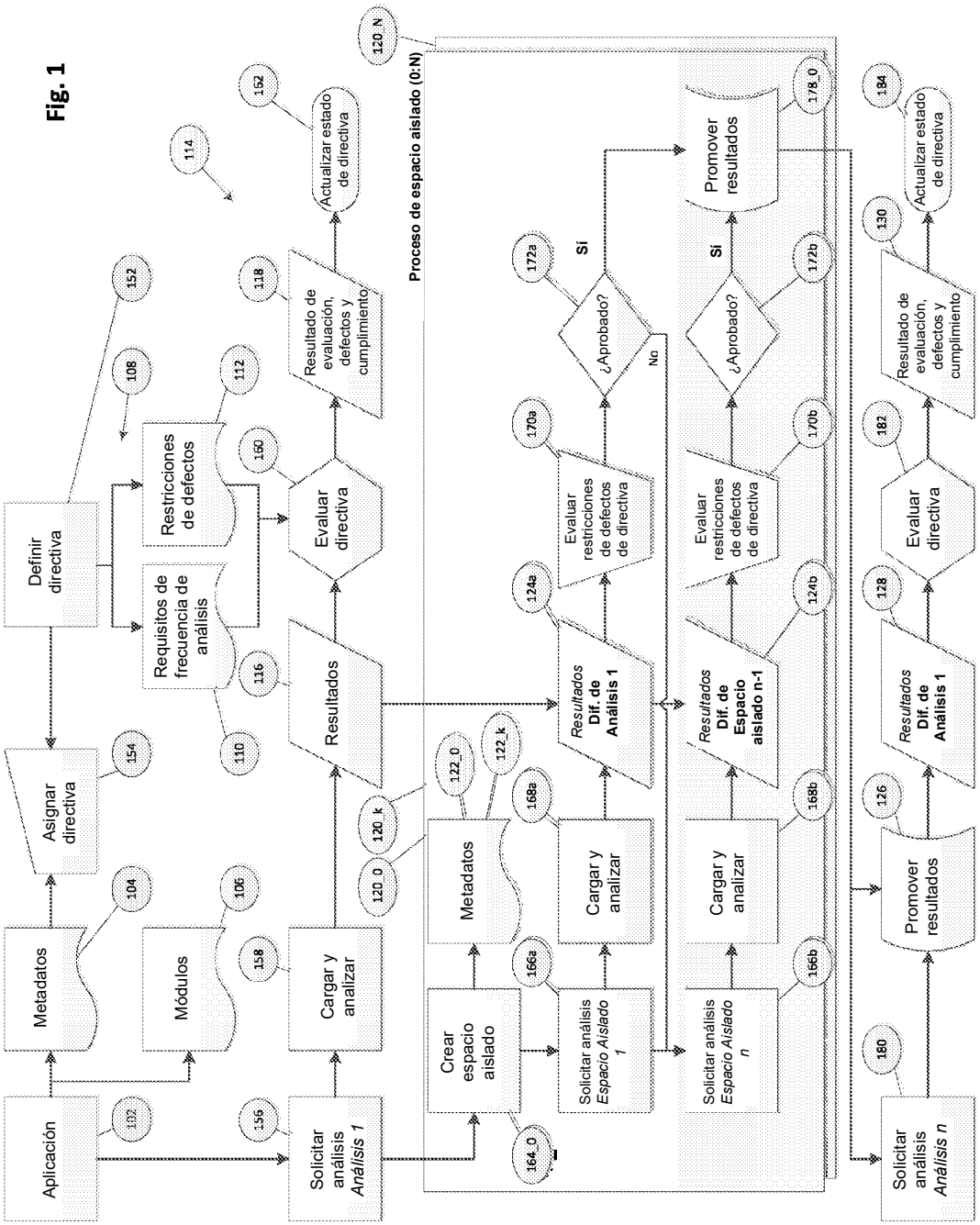
designar un ID de análisis para los resultados de análisis de la aplicación iniciales;
calcular y asociar al ID de análisis un resultado de cumplimiento con base, al menos en parte, en los resultados de análisis de la aplicación iniciales; y
almacenar el resultado de cumplimiento asociado con el ID de análisis en el espacio aislado de directiva.

18. Sistema según la reivindicación 15, donde el servidor está configurado además para:

designar un ID de análisis para los resultados de análisis de aplicación iniciales;
calcular y asociar al ID de análisis un resultado de conformidad con base, al menos en parte, en los resultados de análisis de la aplicación actualizados; y
almacenar el resultado de cumplimiento asociado al ID de análisis en el espacio aislado de directivas.

19. Sistema según la reivindicación 15, donde un único procesador comprende tanto el primer procesador como el servidor.

Fig. 1


Aplicación
Metadatos
Módulos
Asignar directiva
Definir directiva
Restricciones de defectos
Requisitos de frecuencia de análisis
Solicitar análisis Análisis 1
Cargar y analizar
Resultados
Evaluar directiva
Resultado de evaluación, defectos y cumplimiento
Actualizar estado de directiva
Proceso de espacio aislado (0:N)
Crear espacio aislado
Metadatos
Solicitar análisis Espacio Aislado 1
Cargar y analizar
Resultados Dif. de Análisis 1
Evaluar restricciones de defectos de directiva
¿Aprobado?
Sí
No
Solicitar análisis Espacio Aislado n
Cargar y analizar
Resultados Dif. de Espacio aislado n-1
Evaluar restricciones de defectos de directiva
¿Aprobado?
Sí
Promover resultados
Solicitar análisis Análisis n
Promover resultados
Resultados Dif. de Análisis 1
Evaluar directiva
Resultado de evaluación, defectos y cumplimiento
Actualizar estado de directiva