

SISTEMAS Y MÉTODOS PARA ANÁLISIS Y REPORTE DE RED

REFERENCIA CRUZADA A SOLICITUDES RELACIONADAS

Esta solicitud reivindica prioridad de la Sol. de Pat. E.U.A. No. de Ser. 14/523,624, presentada el 24 de Oct. de 2014 y titulada "SISTEMAS Y MÉTODOS PARA ANÁLISIS Y REPORTE DE RED", y la Solicitud de Patente Provisional de E.U.A. No. 62/060,433, presentada el 6 de Octubre de 2014 y titulada "SISTEMAS Y MÉTODOS PARA ANÁLISIS Y REPORTE DE RED," y a la Solicitud de Patente Provisional de E.U.A. No. 62/046,807, presentada el 5 de Septiembre de 2014 y titulada "SISTEMAS Y MÉTODOS PARA ANÁLISIS Y REPORTE DE FLUJO DE RED"; esta solicitud se relacionada con la Solicitud de Patente No Provisional de E.U.A. No. 13/918,633, presentada el 14 de junio de 2013 y titulada "SISTEMAS Y MÉTODOS PARA CONTROL Y CONFIGURACIÓN DINÁMICO DE SEGURIDAD DE RED," el contenido de las cuales se incorpora para referencia en su totalidad.

CAMPO DE LA INVENCION

Las modalidades ejemplares descritas en la presente se refieren a sistemas y métodos para control de seguridad de la red.

ANTECEDENTES DE LA INVENCION

Los arquitectos de seguridad de información y operadores de

seguridad, así como personal de gestión, riesgo y cumplimiento (GRC) todos enfrentan varios retos con respecto a validar que los controles técnicos de seguridad estén en su lugar y funcionando para un recurso o un grupo de recursos dentro del entorno de computación corporativo. Adicionalmente, los sistemas convencionales para el monitoreo y control de la red tienen típicamente capacidad limitada o nada de capacidad para contextualizar la seguridad y datos relevantes de cumplimiento de varios componentes de sistemas de computación, control de seguridad, y/o gestión. Estos retos pueden ser particularmente difíciles en la computación distribuida, sistemas de computación virtualizados, o sistemas de "computación en la nube", donde los componentes y entornos de estos sistemas pueden cambiar frecuente y rápidamente.

Adicionalmente, los sistemas convencionales para el monitoreo y control de la red típicamente usan solo los datos de una fuente individual, o solo un tipo de datos (tales como datos de flujo de la red), excluyendo de esta manera las fuentes potenciales de datos de contexto-soporte importantes y proporcionan una vista céntrica de protocolo de red, unidimensional de flujo de información entre dos sistemas de red.

Las modalidades de la presente descripción ayudan a

abordar estos problemas.

BREVE DESCRIPCIÓN DE LA INVENCION

Entre otras cosas, las modalidades de la presente descripción
5 pueden recolectar y analizar recursos y datos de la red de
múltiples fuentes, y uso de estos datos para presentar una
representación más completa y precisa de las condiciones de
la red entre varios sistemas y aplicaciones de software y las
pólizas que indican la operación de los controles de
10 seguridad en una red comparado con los sistemas
convencionales.

Un método implementado por computadora de acuerdo con
una modalidad de la presente descripción incluye recolectar,
mediante un sistema de computadora, datos de una pluralidad
15 de diferentes tipos de fuentes, en donde los datos
recolectados incluyen datos de la red y datos de recursos;
identificar, mediante el sistema de computadora con base en
los datos de la red en los datos recolectados, un evento de
tráfico de la red y una pluralidad de recursos de la red
20 relacionados con el evento de tráfico de la red; identificar,
mediante el sistema de computadora con base en los datos de
recursos en los datos recolectados, conexiones entre la
pluralidad de recursos de la red; generar, mediante el
sistema de computadora, una gráfica de información de flujo

que representa la pluralidad de los recursos de la red y las condiciones entre la pluralidad de los recursos de la red, en donde la gráfica de información de flujo representa el tráfico de la red que se permite entre los recursos de la red y el tráfico de la red que se bloquea entre los recursos de la red; y presentar la gráfica de información de flujo a través de una pantalla de una interfaz de usuario en comunicación con el sistema de computadora.

La presente descripción incluye métodos y aparatos que llevan a cabo estos métodos, incluyendo sistemas de procesamiento de datos que llevan a cabo estos métodos, y medios legibles por computadora que contienen instrucciones que cuando se ejecutan en los sistemas de procesamiento de datos provocan que los sistemas lleven a cabo estos métodos.

Otras características serán evidentes a partir de las figuras adjuntas y de la descripción detallada que sigue.

BREVE DESCRIPCIÓN DE LOS DIBUJOS

Un entendimiento más completo de ciertas modalidades se puede derivar al referirse a la descripción detallada y a las reivindicaciones cuando se consideran en relación con las siguientes figuras ilustrativas.

La FIGURA 1 representa un entorno de computación ejemplar que se puede usar en conjunción con varias

modalidades de la presente descripción.

La FIGURA 2 representa componentes de control y gestión de seguridad ejemplares de acuerdo con varias modalidades de la presente descripción.

5 La FIGURA 3 representa una representación lógica de varias zonas lógicas de acuerdo con varias modalidades de la presente descripción.

10 La FIGURA 4 es un diagrama de flujo de un método ejemplar de acuerdo con varios aspectos de la presente descripción.

Las FIGURAS 5-7 ilustran el cálculo y visualización de los niveles de cumplimiento de acuerdo con varios aspectos de la presente descripción.

15 La FIGURA 8 es un diagrama de bloques de un sistema ejemplar de acuerdo con varios aspectos de la presente descripción.

La FIGURA 9 es un diagrama de flujo de un método ejemplar de acuerdo con varios aspectos de la presente descripción.

20 La FIGURA 10 es una gráfica de información de flujo ejemplar de acuerdo con varios aspectos de la presente descripción.

La FIGURA 11 es una tabla de datos ejemplar de acuerdo con varios aspectos de la presente descripción.

Las FIGURAS 12-24 son capturas de pantalla que muestran ejemplos de la interacción con una gráfica de información de flujo y tabla de datos de acuerdo con varios aspectos de la presente descripción.

5

DESCRIPCIÓN DETALLADA DE LA INVENCION

Se proporcionan sistemas, métodos y productos de programa de computadora. En la descripción detallada en la presente, las referencias a "varias modalidades", "una modalidad", "una
10 modalidad", "una modalidad ejemplar", etc., indican que la modalidad descrita puede incluir un aspecto, una estructura o característica particular, pero cada modalidad no puede incluir necesariamente el aspecto, estructura o característica particular. Por otra parte, estas frases no
15 están necesariamente refiriéndose a la misma modalidad. Además, cuando un aspecto, estructura o característica particular se describe en relación con una modalidad, se afirma que está dentro del conocimiento de la persona experta en la técnica para llevar a cabo este aspecto, estructura,
20 característica en relación con otras modalidades ya sea no explícitamente descritas. Después de la lectura de la descripción, será evidente para una persona experta en la técnica(s) relevante como implementar la descripción en las modalidades alternativas.

En varias modalidades, los métodos descritos en la presente se implementan usando las diversas máquinas particulares descritas en al presente. Los métodos descritos en la presente se pueden implementar usando las siguientes
5 máquinas particulares, y aquellas desarrolladas a partir de ahora, en cualquier combinación adecuada, como se apreciaría inmediatamente por una persona experta en la técnica. Además, como es claro a partir de esta descripción, los métodos descritos en la presente pueden dar por resultado varias
10 transformaciones de ciertos artículos.

Por razones de brevedad, la red de datos convencional, desarrollo de aplicación y otros aspectos funcionales de los sistemas (y componentes de los componentes operativos individuales de los sistemas) no se pueden describir con
15 detalle en la presente. Adicionalmente, las líneas de conexión mostradas en las diversas figuras contendidas en la presente se proponen para representar relaciones funcionales ejemplares y/o acoplamientos físicos entre los diversos elementos incluyendo, por ejemplo, corrientes de eventos
20 tales como alimentaciones de datos IPFIX, canales de datos, inspección de la red directa (tal como en un sistema de detección de intrusión), alimentaciones de registros, inspección de registros, e/o interacciones programáticas tales como aquellas que utilizan una interfaz de programación

de aplicación. Cabe destacar que muchas relaciones funcionales alternativas o adicionales o conexiones físicas pueden estar presentes en un sistema práctico.

La presente descripción puede referirse a los siguientes
5 términos definidos en la siguiente lista. Las definiciones en esta lista son ejemplares solamente. Los cambios, modificaciones, y variaciones basados en las diferentes definiciones de los términos, así como diferentes términos, se proponen para ser incluidos dentro del alcance de la
10 presente descripción.

Recurso- un hardware discreto con base en el sistema de computación virtualizado que procesa datos en el centro de datos, una computadora virtualizada o máquina virtual. Los recursos pueden ser un miembro de una Zona de Confianza ya
15 sea a través de métodos automatizados como se expresa en las pólizas de membresía o manualmente a través de una acción del usuario.

Atributo del recurso - una propiedad de un recurso que incluye pero no se limita a cualquier ajuste de configuración
20 de sistema operativo, aplicación de procesamiento de datos desplegado en el recurso, ajuste de configuración de aplicación, componente del sistema basado o actualizado en el hardware incluyendo interfaz de red, memoria, disco, interconexión de componente de red, identificador único,

nombre, o cualquier componente o etiqueta de datos discreto asociado con un recurso, una configuración de recursos, o la posición del recurso dentro del sistema del centro de datos físico virtualizado.

5 Control técnico de seguridad - un dispositivo, tecnología, programa de software, o una configuración o atributo de un elemento que lleva a cabo una función de seguridad o cambia la postura o estado de seguridad de un elemento que incluye pero no se limita a: servidor de
10 seguridad, detección y prevención de intrusiones, escaneo de vulnerabilidad, gestión y mitigación de vulnerabilidad, anti-software maligno, detección y prevención de intrusión con base en anfitrión, monitoreo de la integridad de archivos, autenticación - autorización - auditoría, encriptación en
15 movimiento, encriptación en reposo, encriptación de la gestión de clave y ficha digital, gestión de derechos del usuario, control de acceso de la red, especificación de longitud de la contraseña, ajustes de configuración que indican la operación de un sistema o elemento en uno u otro
20 contexto de varios niveles de seguridad.

Póliza- una póliza es una regla, conjunto de reglas, y/o conjunto de datos usados para guiar la operación o comportamiento de un sistema o componente/elemento de sistema. Específicamente un cuerpo de datos asociado con un

control de técnico de seguridad que indica el comportamiento y función de ese control.

Zona lógica - un agrupamiento arbitrario de recursos que pueden o no tener atributos comunes asociados con un conjunto
5 de pólizas.

Hipervisor - una pieza de software de computadora, firmware o hardware que crea y ejecuta máquinas virtuales.

Conmutador virtual- una pieza de software que proporciona la interconexión de red de máquinas virtuales en
10 un hipervisor.

Servidor de seguridad- un control técnica de seguridad con base en software o hardware que controla el tráfico de red que pasa a través de él al analizar los componentes de tráfico (paquetes) y hacer una decisión o dejar pasar o
15 bloquear el tráfico con base en un conjunto de reglas.

Sistema de Prevención de Intrusión (IPS) - un control técnico de seguridad con base en software o hardware que inspecciona las condiciones de la red para el propósito de detectar e interrumpir el tráfico de la red indeseable que en
20 las firmas o modelación de comportamiento.

Escáner de Vulnerabilidad - un control técnico de seguridad con base en software o hardware que evalúa el estado de vulnerabilidad de los recursos en la red a través del proceso de conectarse al recurso sobre la red o ejecutar

el recurso como un proceso y evaluar el recurso con base en las firmas de vulnerabilidad conocidas, indicadores de vulnerabilidad, comportamientos observados del recurso, programas que se ejecutan en el recurso y/o atributos operacionales del recurso.

Marco de Conformidad- un conjunto estructurado de directrices, procesos y procedimientos publicados para el propósito de definición de acuerdo con las regulaciones, especificación o legislaciones establecidas.

10 Zona de Confianza Catbird - una construcción de zonificación lógica que consiste de la recolección de pólizas que incluyen pólizas de configuración de control, pólizas de membresía, y recolección de métodos que implementan la reconfiguración de control dinámica en respuesta a los cambios en el entorno de computación.

GRC - Riesgo de Gestión y Cumplimiento, un agrupamiento generalizado de tres funciones relacionadas dentro de una organización que tratan respectivamente con la gestión corporativa, la gestión de riesgo empresarial (ERM) y cumplimiento corporativo con leyes y regulaciones aplicables.

Las modalidades de la presente descripción pueden monitorear todos los cambios de los atributos de recursos (es decir, aquellos recursos dentro o fuera de una Zona de Confianza), cambios de entorno de computación, cambios de

componentes de la red, eventos de control de seguridad, eventos de componente de gestión, eventos de recursos, y/o eventos de la red. Estos eventos, que pueden ser referidos colectivamente como “eventos ambientales” en la presente, se
5 pueden monitorear dentro del contexto de todas las pólizas de configuración de control tal que cualquier póliza de configuración de control se puede modificar dinámicamente para asegurar que el control esté aún en efecto de cualquier recurso en una Zona de Confianza respectiva.

10 Los eventos ambientales dentro del contexto de los miembros de la Zona de Confianza y la póliza de membresía se puede monitorear tal que diferentes conjuntos de pólizas de control de seguridad se pueden asignar dinámicamente a, o cambiar para, cualquier recurso en una Zona de Confianza al
15 mover el recurso de una Zona de Confianza a otra o al cambiar una póliza o pólizas para una Zona de Confianza de la cual ese recurso es un miembro. Estos cambios se pueden aplicar a múltiples recursos al llevar a cabo simultáneamente la misma acción de movimiento en múltiples recursos, particularmente
20 en el caso de un cambio de la membresía de la Zona de Confianza.

Con referencia ahora a la FIGURA 1, se representa un entorno de computación ejemplar 100 que puede operar en conjunción con las modalidades de la presente descripción.

Los componentes del entorno 100 se pueden implementar usando cualquier combinación deseada de componentes de hardware y software, y se pueden alojar por, por ejemplo, el sistema de computación anfitrión 810 representado en la FIGURA 8.

5 Alternativa o adicionalmente, el sistema 800 (o cualquier porción del mismo) se puede incluir en el entorno 100. En el ejemplos mostrado en la FIGURA 1, el entorno 100 incluye cuatro tipos diferentes de componentes: elementos de computación (CE), elementos de red (NE), elementos de gestión

10 (ME), y elementos de seguridad (SE). Las modalidades de la presente descripción pueden interactuar con cualquier número de esos componentes, así como otros componentes. Cada componente individual puede representar computadoras o máquinas virtuales incluyendo cualquiera de los recursos de

15 computación de hardware físicos o virtualizados deseados, tales como procesadores, memorias, conmutadores, enrutadores, equilibradores de carga, sistemas operativos, aplicaciones de software, y/o elementos de configuración (archivos, procesos, pólizas, programas). Cualquier elemento o derivado del mismo

20 representado en la FIGURA 1 se puede implementar usando cualquier combinación deseada de componentes físicos y virtuales. Los elementos virtualizados se pueden unir al hardware físico usando cualquier software de hipervisor deseado, tal como VMware ESXi, Microsoft Hyper-V, y/o

OpenStack.

Los elementos de computación se caracterizan por su función como plataformas de aplicación dedicadas al procesamiento de datos y al proporcionar servicios de
5 computadora en la forma de aplicaciones a una población de usuarios de varios niveles de privilegio. Un ejemplo de un elemento de computación puede incluir un servidor de Microsoft Windows físico virtualizado o servidor Linux que ejecuta una aplicación.

10 Los elementos de red se caracterizan por su función para proporcionar la interconectividad (en parte o en totalidad) de varios elementos dentro del entorno de computación con la tecnología de red protocolos y para proporcionar el transporte de datos entre los elementos del entorno de
15 computación. Los ejemplos de elementos de red pueden incluir enrutadores, conmutadores, conmutadores neutralizados, redes, VLANs, y/o componentes de red definidos por software incluyendo LANs extensibles virtuales (VXLANS).

Los elementos de gestión se caracterizan por su función
20 como aplicaciones anfitrionas que se dedican a la gestión y operación del entorno de computación, el procesamiento de datos, y proporcionan servicios de gestión operacionales en la forma de aplicaciones de gestión y operación a una población de usuarios administrativos privilegiados. Los

elementos de gestión pueden gestionar otros elementos incluyendo elementos de computación, elementos de la red u otros elementos de gestión. Un ejemplo de un elemento de gestión puede incluir un servidor Microsoft Windows que ejecuta el software VMware vSphere Server que está gestionando los hipervisores en el entorno de computación.

Los elementos de seguridad se caracterizan por su función de proporcionar implementaciones de varios controles de seguridad técnicos ya sea en el nivel de la red, anfitrión, máquina virtual, recurso, programa, o proceso. Los elementos de seguridad pueden tener arquitecturas de despliegue jerárquicas que incluyen cualquier número deseado de elementos de la red, elementos de gestión, elementos de computación, programas, procesos, y métodos implementados en un formato físico y/o virtualizado. Los ejemplos de los elementos de seguridad pueden incluir un dispositivo de servidor de seguridad y su elemento o software de gestión, software antivirus y sus mecanismos de gestión y actualización, un escáner de vulnerabilidad, y/o una infraestructura de clave pública centralizada utilizada para derechos de acceso o usuario.

La FIGURA 2 representa componentes y entradas y salidas programáticas de un Sistema de Gestión de Control de Seguridad (SCMS) de acuerdo con una modalidad de la

presente descripción. Esta modalidad puede incluir varios componentes de hardware y software, algoritmos de software, estructuras de datos, y bases de datos para implementar varias funciones del SCMS 200. Los SCMS's alternos pueden
5 tener más, menos o diferente componentes y funcionalidad.

En la modalidad ejemplar representada en la FIGURA 2, el SCMS 200 interactúa con el entorno de computación a través de los mecanismos de mensajería programáticos implementados a través de una o más interfases estandarizadas y/o
10 propietarias o Interfases de Programación de Aplicación (APIs). La interfaz puede utilizar la encriptación de Capa de Conexión Segura (SSL), así como cualquiera de otras técnicas de encriptación deseadas para asegurar la privacidad e integridad de los mensajes, eventos, directivas y comandos.
15 Las técnicas de encriptación utilizadas por las modalidades de la presente descripción pueden incluir autenticación mutua para los elementos de envío y recepción. Los mecanismos de mensajería programáticos se pueden implementar de cualquier manera adecuada o las modalidades ejemplares de la presente
20 descripción tal como a través de APIs, integraciones de interfaz de línea de comando, consultas de base de datos, recolección programática de datos de visualización (es decir, adaptación de pantallas), métodos de comunicación y proceso, acceso de sistema de archivos y otros.

A través de los mecanismos de mensajería programáticos, el SCMS 200 descubre la información acerca del entorno de computación. Esta información puede incluir información relacionada con elementos individuales, o combinaciones de elementos, o todos los elementos. La información descubierta se puede usar por el SCMS 200 para cualquier propósito deseado, tal como para identificar elementos que se aseguran por el sistema y/o para determinar heurísticamente atributos de elementos para configurar los controles técnicos de seguridad. La información descubierta también se puede usar para evaluar el cumplimiento con las regulaciones gubernamentales o industriales, postura de seguridad, función de control de seguridad, eficacia del control de seguridad, cobertura de control de seguridad y/u operación de control de seguridad.

Los mecanismos de mensajería programáticos pueden incluir (donde es soportado por el elemento o elementos) el intercambio entre el elemento o elementos y el SCMS 200, los mensajes relacionados con el elemento, registros, telemetría, ajustes de configuración, datos generados por los programas o procesos que incluyen o no incluyen el SCMS 200, atributos de elementos, datos que reflejan el estado y configuración actual del elemento, y cualquiera de otros datos relevantes para los controles técnicos de seguridad, pólizas o

referencias, ya sea relativas al mismo elemento o como disponible del elemento u otros elementos en el entorno de computación, todos de los cuales se pueden referir colectivamente en la presente como "eventos".

5 Los mecanismos de mensajería programáticos también pueden incluir una interfaz de comando y/o configuración para reconfigurar el elemento en términos de ajuste de configuración, pólizas, archivos de configuración, el inicio y detención de los componentes del elemento incluyendo
10 programas procesos, y/o para comandos de problema directamente al elemento para el propósito de cambiar el estado operacional del elemento para iniciar las reconfiguraciones llevadas a cabo a través del mismo mecanismo, todos de las cuales se pueden referir
15 colectivamente en la presente como "directivas".

En la modalidad ejemplar representada en la FIGURA 2, los diversos componentes pueden incluir cualquier combinación deseada de componentes de hardware y/o software para llevar a cabo varias funciones. Por ejemplo, el componente de
20 Procesamiento y Cuestión de Eventos puede normalizar o transformar estos eventos para archivado y procesamiento adicional por otros componentes. Las normalizaciones y transformaciones pueden incluir sustitución o adición de atributos de recursos a través de la adición de

identificadores relevantes de recursos para el propósito de asociar los eventos con un recurso de información, la remoción de los datos del evento para la reducción de espacio para propósitos de archivo, la adición de los atributos
5 determinados por el sistema para ser relativos con el elemento de origen a través de eventos o salidas algorítmicas del sistema generado de los eventos que se originan de otros elementos. El procesamiento de eventos puede incluir extraer, del evento, corrientes de datos de información relevante para
10 la creación, mantenimiento y ejecución de pólizas, identificación de recursos, configuración de controles técnicos de seguridad, y datos relevantes al elemento y el estados del elemento con respecto a las referencias o líneas bases consistentes con en que impactan el nivel de
15 cumplimiento con las referencias o líneas bases.

La Creación y Configuración de la Zona Lógica lleva a cabo las tareas relacionadas con la creación y configuración de la Zona de Confianza. Este componente trata con el mapeo de los recursos de información para las zonas lógicas (Zonas
20 de Confianza) y proporciona la asociación de las pólizas de control técnicas de seguridad para el recurso de información.

El componente de Lógica y Heurística de Póliza y referencia lleva a cabo el análisis de las pólizas y configuraciones de los controles técnicos de seguridad,

relevantes a y dentro del contexto de las zonas lógicas y los recursos de información dentro de ellos dentro del contexto de las corrientes de eventos de elementos. Estos datos de gestiones de componentes contenidos en los eventos para el
5 propósito de validar los controles que aún están en su lugar y mapear aquellas validaciones de control a varios marcos de conformidad tales como PCI DSS 2.0, HIPAA, COBIT 4.1, DIACAP, y/o FISMA, así como marcos arbitrarios, tales como aquellos ideados en la discreción de un operador a través de la
10 especificación de varias combinaciones de: pólizas, controles técnicos, atributos de recursos, interacciones requeridas con el SCMS verificado por los eventos, y/o atributos de elementos de varios tipos, tales como aquellos representados en la FIGURA 1. Esta lógica evalúa los cambios en la
15 configuración de control técnico de seguridad y los atributos de recursos y lleva a cabo las reconfiguraciones de póliza de control técnicas de seguridad basadas en aquellos cambios de atributos de recursos para el propósito de mantener la póliza y aplicación de los controles técnicos de seguridad y la
20 conformidad con la referencia. Esta lógica evalúa los diversos ajustes de póliza y toma las acciones apropiadas en respuesta a los cambios de atributos de recursos y a los cambios de membresía de la Zona de Confianza del recurso.

El componente de Gestión de Control y Directivas lleva a

cabo la construcción de las directivas e inicia el envío de las directivas a los elementos de entorno de computación para llevar a cabo la acción o acciones apropiadas de los elementos incluyendo: la generación de eventos, transferencia
5 de datos de configuración y proceso en cualquier dirección, el inicio y detención de un control técnico de seguridad, la reconfiguración del control técnico de seguridad con una póliza actualizada, la reconfiguración de un elemento de cualquier tipo, el inicio y detención de un programa o
10 proceso, el cambio de una configuración o atributo que afecta una configuración, y al validación de que el control se aplica a cualquier recurso de información como es calificado por los datos de configuración suministrados a través de los eventos o directivas.

15 La Base de Datos del Evento es una base de datos usada para el almacenamiento, recuperación, y gestión de eventos de cualquiera y todos los elementos incluyendo el mismo software de control de seguridad. Esta base de datos se usa para almacenar y consultar subsecuentemente los eventos para los
20 datos de atributos de recurso, datos de configuración de control de seguridad, datos de póliza y datos de evento para los propósitos de los diversos bloques lógicos y heurística implementada en los componentes.

La Base de Datos de Recursos/Atributos se usa para el

almacenamiento, recuperación, y gestión de recursos y datos de atributos de recursos. Esta base de datos se usa para almacenar y consultar subsecuentemente los recursos y datos de atributos de recursos para los propósitos de los diversos bloques lógicos y heurística implementada en otros componentes.

La Base de Datos de la Zona de Confianza es un componente de base de datos usado para el almacenamiento, recuperación, y gestión de zonas lógicas (Zonas de Confianza). Este componente se usa para almacenar y consultar subsecuentemente, actualizar, modificar las Zonas de Confianza, los recursos de información dentro de una Zona de Confianza, las pólizas de control técnicas de seguridad asociadas con la Zona de Confianza, para los propósitos de los diversos bloques lógicos y heurística implementada en otros componentes.

La Base de Datos de la Póliza es un componente de base de datos usado para el almacenamiento, recuperación, y consulta, y gestión de pólizas para los controles técnicos de seguridad, recursos, modalidades de implementación de software de la presente descripción (o porciones de las mismas), y el entorno.

La FIGURA 3 representa la representación lógica de las Zonas Lógicas, también referidas como en la presente Zonas de

Confianza. Esta construcción de configuración, con sus estructuras de datos asociados, une los recursos y grupos de recursos a través de la aplicación de pólizas que indican la función y comportamiento de los controles técnicos de seguridad. Las Zonas de Confianza pueden tener números arbitrarios de recursos y pólizas de control técnicas de seguridad. Los diferentes controles técnicos de seguridad pueden tener construcciones de póliza que permiten la herencia jerárquica o lógica de/con otras pólizas de modo que la representación de una póliza de Control-N representa la recolección de todas las pólizas de configuración de control técnicas de seguridad, archivos, datos, ajustes de configuración que especifican la operación específica del control técnico de seguridad en cualquier momento, almacenado como una unidad para el control técnico de seguridad N.

Mientras que el número de pólizas de control pueden ser contingentes en el número de controles técnicos de seguridad soportados, se pueden integrar nuevos controles con las modalidades de la presente descripción ya que tales controles se desarrollan y están disponibles, y pueden resultar de la combinación de los datos funcionales de control y los eventos de varios controles técnicos de seguridad. Por consiguiente, el número de pólizas de control puede variar con base en los requisitos de seguridad para el entorno de computación y los

controles de seguridad técnicos disponibles y configurados.

Las pólizas de membresía de la Zona de Confianza pueden indicar como los recursos se colocan automáticamente en una o más Zonas de Confianza basadas en los atributos de recursos y eventos que se originan de cualquier elemento como el recolectado por el SCMS. Cada recurso se puede evaluar, ya que los eventos que indican un atributo de recurso se han cambiado se reciben por el software de control de seguridad, dentro del contexto de todas las pólizas de membresía de la Zona de Confianza para afectar un cambio de membresía de la Zona de Confianza al mover el recurso de una Zona de Confianza a otra o al agregar el recurso a otra Zona de Confianza.

Cualquier combinación y/o subconjunto de los elementos de los métodos representados en la presente se puede practicar en cualquier orden adecuado y en conjunción con cualquier sistema adecuado, dispositivo, y/o proceso. Los métodos descritos y representados en la presente se pueden implementar de cualquier manera adecuada, tal como a través del software de control de seguridad que opera en uno o más sistemas de computadora, incluyendo el sistema anfitrión representado en la FIGURA 8. El software de control de seguridad puede comprender instrucciones legibles por computadora almacenadas en un medio legible por computadora

tangible (tal como la memoria 814 del sistema de computadora anfitrión 810) y se puede ejecutar por uno o más procesadores (tal como el procesador 812 del sistema de computadora anfitrión 810) para llevar a cabo los métodos de las diversas
5 modalidades.

La FIGURA 4 representa un proceso ejemplar de acuerdo con varias modalidades de la presente descripción. En la FIGURA 4, el método 400 incluye identificar uno o más recursos asociados con una o más zonas lógicas (405),
10 establecer conexiones con uno o más componentes (410), asociar una o más pólizas de seguridad con una o más zonas lógicas (415), detectar los cambios en uno o más atributos para uno o más recursos (420), detectar las vulnerabilidades de seguridad y correcciones a las mismas (425), cambiar las
15 membresías de zona para uno o más recursos (430), modificar uno o más ajustes de configuración de servidor de seguridad (435), asociar una o más pólizas de conformidad con una o más zonas lógicas (440), analizar las modificaciones a los ajustes de configuración del servidor de seguridad (445),
20 determinar uno o más niveles de conformidad (450), y mostrar uno o más niveles de conformidad (455). Los pasos del método 400 se pueden implementar (en totalidad o en parte, y en cualquier orden deseado) por el software que opera en un sistema de computadora, tal como el sistema de computación

anfitrión ejemplar 810 representado en la FIGURA 8.

Las modalidades de la presente descripción pueden identificar cualquier número de diferentes recursos (405) asociados con cualquier número de diferentes zonas lógicas, tales como los recursos en las Zonas lógicas 1 y 2 representadas en la FIGURA 2. Como se plantea en lo anterior, estos recursos pueden incluir cualquier combinación de componentes físicos y virtuales.

Las conexiones se pueden establecer (410) con cualquier número de diferentes componentes de software y hardware. Las modalidades de la presente descripción pueden operar en conjunción con varios mecanismos de mensajería programáticos que ayudan a unir el SCMS con los controles técnicos de seguridad dentro del entorno. Las zonas lógicas, o Zonas de Confianza, se pueden crear de cualquier manera adecuada, tal como a través de interacciones con los componentes lógicos no representados, pólizas colocadas en una o más zonas lógicas que son relevantes a los controles técnicos de seguridad unidos al SCMS.

Los eventos del entorno de computación se pueden recibir a través de mecanismos de mensajería programáticos que proporcionan información variada acerca del entorno, incluyendo los recursos que son protegidos por los controles técnicos de seguridad y/o el estado de los controles técnicos

de seguridad. Las conexiones entre el software de control de seguridad y varios componentes (tales como componentes de gestión) se pueden hacer para enviar y recibir información, detectar cambios en los atributos de varios recursos, y
5 controlar y configurar varios sistemas, tal como un servidor de seguridad que protege uno o más recursos o zonas lógicas.

En una modalidad, las características de implementación del software de control de seguridad de la presente descripción estable conexiones a través de los mecanismos de
10 mensajería programáticos (como se describe en lo anterior) entre ellos y el elemento de gestión o el componente de gestión de recursos de una infraestructura virtualizada, tal como un servidor VMware vSphere, y entre él y el elemento de gestión para un servidor de seguridad virtualizado
15 implementado en la misma infraestructura virtualizada, tal como un servidor de seguridad VMware vCNS App. Los cambios en el atributo de un recurso se pueden detectar a través de una comunicación con el elemento de gestión y el software de control de seguridad.

20 Los recursos, y cambios en los atributos de los recursos, se pueden detectar al consultar periódicamente el elemento de recurso u otros componentes de hardware o software. Por ejemplo, el control técnico de seguridad, referido en la presente como un Monitor de Infraestructura

Virtual (VIM), puede usar la conexión al servidor vSphere para identificar y enumerar todos los elementos de computación virtualizados (es decir, máquinas virtuales) y todos los conmutadores virtuales. A través de la interfaz API con vSphere, el software de control de seguridad que implementa las características de la presente descripción puede consultar periódicamente y re-enumerar las máquinas virtuales configuradas y los conmutadores virtuales, determinado de esta manera la creación de nuevos recursos (tal como las máquinas virtuales y los conmutadores virtuales) o cambios a los atributos de los recursos existentes al comparar los resultados de las consultas subsecuentes con la consulta previa. Los atributos para una pluralidad de diferentes recursos controlados por un componente de gestión de recursos se pueden monitorear al consultar el componente de gestión de recurso, así como a través de comunicaciones originadas por el componente de gestión de recursos al software de control de seguridad.

El VIM también es capaz de consultar varias configuraciones de máquina virtual y ajustes tal como el Identificador Universalmente Único (UUID) de infraestructura virtual par la máquina virtual, las tarjetas de interfaz de red virtuales, la dirección del Protocolo de Internet de tarjeta de interfaz de máquina (IP), posición actual de la

tarjeta de la interfaz de la máquina virtual dentro del conmutador virtual o conmutadores, y muchos más ajustes de configuración, que se pueden referir en la presente colectivamente como "atributos de la máquina virtual". A través del procesamiento de eventos generador por VIM, el SCMS "introduce" en cada máquina virtual como un recurso de información dentro de SCMS, almacenar los datos de recursos incluyendo los atributos en la base de datos de Recurso/Atributos.

10 En la presente modalidad ejemplar, la disponibilidad de un elemento de gestión que proporciona a la interfaz API de enumerar recursos y atributos de recursos hace este proceso programáticamente simplificado cuando el entorno de computación incluye una infraestructura predominantemente virtualizada. Las modalidades alternas podrían recolectar y/o
15 crear los mismos datos similares, con respecto a los elementos de computación físicos a través del establecimiento de los mecanismos de mensajería programáticos con una variedad o combinación de elementos de gestión, otros
20 controles de seguridad técnicos (tales como escáneres de red), y con los mismos elementos de computación físicos. De esta manera, las modalidades de la presente descripción pueden operar con cualquier combinación de componentes físicos y virtuales.

El sistema puede instanciar otra conexión con el elemento de gestión para el servidor de seguridad virtualizado (es decir, un componente de gestión de servidor de seguridad) implementado en la misma infraestructura virtualizada. Esta conexión no necesita incluir necesariamente un control de seguridad técnico en sí mismo, sino más bien una interfaz programática al servidor de seguridad (un control de seguridad técnico). La funcionalidad desde el servidor de seguridad se puede gestionar a través de una comunicación entre el software de control de seguridad del componente de gestión del servidor de seguridad. En modalidades ejemplares, la interfaz programática o API permite que el SCMS controle completamente el servidor de seguridad, la operación del servidor de seguridad y las pólizas del servidor de seguridad expresados en los ajustes de configuración y las listas de control de acceso (ACLs), a través de una combinación de directivas expedidas y eventos recolectados para y del elemento de gestión del servidor de seguridad. Esta conexión y el API constituyen un control técnico de seguridad orquestado con respecto al SCMS.

Se pueden asociar varias pólizas de seguridad con diferentes recursos y/o zonas lógicas (415) de cualquier manera adecuada. Por ejemplo, un operador del SCMS, así como el software de control del software mismo, pueden crear y

configura varias zonas lógicas, y las pólizas de seguridad para estas zonas, expresadas como una secuencia de reglas. En una modalidad ejemplar, las reglas pueden tener la forma:

Puerto de protocolo Fuente_Zona de ConfianzaA

5 Destination_Zona de ConfianzaB [permitir, negar]

En este ejemplo, cada regla es una regla de Control de Acceso de Zona, y el conjunto de todas las reglas de Control de Acceso de Zona configuradas se pueden referir en la presente como una lista de Control de Acceso de Zona o ZACL. En el

10 ejemplo anterior, la Zona de Confianza de origen es nombrada Zona de ConfianzaA y la Zona de Confianza de destino es nombrada Zona de ConfianzaB. Al proporcionar esta abstracción, las modalidades de la presente descripción ayudan a simplificar la gestión de lo que es conocido por los

15 profesionales de la seguridad de la red como Listas de Control de Acceso, que consisten típicamente de direcciones IP de origen y destino. Mientras que los atributos de recursos complejos y desasociados similares a la dirección IP se usan dentro de los ACLs convencionales, en los ZACLs

20 utilizados por las modalidades de la presente descripción, la fuente y destinos son zonas lógicas que tienen nombres legibles por humanos que son más identificables con respecto a la información de los recursos en los ZACLs que están protegiéndose con el control técnico de seguridad del

servidor de seguridad. Con referencia nuevamente a la FIGURA 3, cada Zona de Confianza se puede asociar con una póliza (415) para el control técnico de seguridad del servidor de confianza ya que la Zona de Confianza se coloca en el ZACL (por ejemplo, a través de agregar una regla de Control de Acceso de Zona que contiene la Zona de Confianza al ZACL), mediante lo cual los cambios en la configuración al servidor de seguridad se llevan a cabo de acuerdo con la póliza. La póliza de seguridad también se puede evitar o reemplazar por cualquier Zona de Confianza ya colocada en el ZACL, por ejemplo, al modificar la regla de Control de Acceso de Zona.

El software de control de seguridad puede monitorear los cambios (420) para todas las máquinas virtuales y los componentes físicos dentro de una o más zonas lógicas. Los datos de eventos se pueden analizar y procesar, y los controles técnicos de seguridad se pueden configurar o reconfigurar (435) a través de la modificación de las pólizas. La modificación de los ajustes de configuración para el servidor de seguridad se puede hacer basada en un cambio en un atributo individual de un recurso individual, así como con base en análisis de varios cambios de atributos para varios recursos. Por ejemplo, con referencia nuevamente a la FIGURA 3, en caso donde las membresías de la Zona Lógica para un recurso en la Zona Lógica 1 y un recurso en la Zona Lógica

2 se cambian, el software de control de seguridad puede analizar el cambio en la membresía de la zona por ambos recursos y hacer un cambio individual a los ajustes de configuración para el servidor de seguridad de acuerdo con el
5 análisis. Entre otras cosas, considerando varios cambios de atributos (tal como el cambio en la membresía de la zona anterior) juntos pueden ayudar a las modalidades de la presente descripción a evitar las modificaciones repetitivas y falsas para el servidor de seguridad.

10 Continuando con el ejemplo anterior, cuando un operador o software pone un recurso (Recurso1) en la Zona de ConfianzaA el software de control de seguridad detecta el cambio en los atributos del recurso (420), particularmente el cambio en la membresía de la Zona de Confianza, y modifica la
15 configuración del servidor de seguridad (435) por consiguiente. En este ejemplo, como resultado del cambio de la Zona de Confianza, el software de control de seguridad evalúa la dirección IP de atributo de recurso para el Recurso1 y después implementa un ACL en el servidor de
20 seguridad en la forma nativa del servidor de seguridad (ACL), a través de una directiva formulada al servidor de seguridad. Si un segundo recurso (Recurso2) se pone en la Zona de ConfianzaB, el software de control de seguridad detecta el cambio (420), evalúa la dirección IP atribuida de recursos

para el Recurso2, y después implementa un ACL en el servidor de seguridad (435) en la forma nativa del servidor de seguridad (ACL) a través de una directiva formulada al servidor de seguridad. En este punto, se asume que se desea
 5 que todas las conexiones del Protocolo de Control de Transmisión (TCP) entre la Zona de ConfianzaA y la Zona de ConfianzaB se niegue, la regla del servidor de seguridad nativo (ACL) puede presentarse como:

Asset1_IP_address Asset2_IP_address TCP cualquiera se
 10 niega

Y el ZACL puede presentarse como:

Zona de ConfianzaA Zona de ConfianzaB TCP cualquier
 negación

Para cada recurso agregado ya sea Zona de ConfianzaA o
 15 Zona de ConfianzaB, el sistema puede continuar construyendo el servidor de fuego nativo ACL a través de directivas subsecuentes configurando el servidor de seguridad automáticamente conforme el operador puebla las Zonas de Confianza con recursos.

20 Las modalidades de la presente descripción pueden operar para detectar cualquier cambio deseable en los atributos de un recurso, tal como la dirección de protocolo de internet (IP) del recurso. Por ejemplo, si una dirección IP del Protocolo de Configuración de Anfitrión Dinámico (DHCP) se

deja expirar y el Recurso1 recibe una dirección IP diferente en la renovación del último; o el Recurso1 recibe una dirección IP diferente a través de DHCP después de ser desactivado con un período de tiempo; o un hacker (pirata informático) cambia la dirección IP en un esfuerzo de derivar los controles de acceso de la red; o un administrador asigna accidentalmente la dirección IP errónea (escribe más), en todos los casos, la dirección IP del Recurso1 cambia. Debido a que el software de control de seguridad de la presente descripción está monitoreando los atributos de recurso de todos los recursos (por ejemplo, a través de VIM), cuando se detecta un cambio del atributo del recurso (420), el software de control de seguridad puede formular y enviar una directiva (435) para modificar el ACL en el servidor de seguridad para reflejar la nueva dirección IP.

Se considerará ahora una tercera Zona de Confianza, Zona de ConfianzaC, de la cual el operador desea permitir todas las conexiones TCP a la Zona de ConfianzaB. La ZACL para estas pólizas podría verse como esto:

20 Zona de ConfianzaA Zona de ConfianzaB TCP cualquier
negación

 Zona de ConfianzaC Zona de ConfianzaB TCP cualquier
permisión

En un ejemplo que utiliza estas Zonas de Confianza,

considerar que, como resultado de un cambio arquitectónico, el Recurso1 (actualmente en la Zona de ConfianzaA) ahora necesita ser dejado que haga cualquier conexión TCP al Recurso2 (actualmente en la Zona de ConfianzaB). El Recurso1
5 se puede mover de la Zona de ConfianzaA a la Zona de ConfianzaC. El sistema a través de su monitoreo de los atributos de recursos, detecta el movimiento (420) y puede formular una directiva para el servidor de seguridad (435) para remover la dirección IP del Recurso1 de la negación de
10 ACL y agregar la dirección IP del Recurso1 para permisión de ACL. Esto puede dar por resultado cambiar completamente la póliza del servidor de seguridad para tanto Recurso1 como Recurso2, y se puede llevar a cabo automáticamente, con esfuerzo del operador mínimo, y sin la necesidad de manipular
15 ACL numéricas complejas en el servidor de seguridad. De esta manera, los ajustes de configuración del servidor de seguridad se pueden modificar en respuesta a la detección del movimiento de un recurso de una zona lógica a otra para permitir o prevenir o impedir la comunicación entre el
20 recurso movido y otro recurso o componente.

Entre otras cosas, la zonificación lógica con las Zonas de Confianza ayuda a mantener, para el servidor de seguridad de control técnico de seguridad, la póliza y la integridad de la póliza cuando los atributos de recurso que impactan la

operación del servidor de seguridad se cambian por razones naturales, accidentales o maliciosa. Adicionalmente, las modalidades de la presente descripción son igualmente eficaces en reconfigurar los ajustes de un servidor de seguridad cuando un recurso (tal como un componente de hardware físico) mueve físicamente las ubicaciones, o se reasigna simplemente de una zona lógica a otra sin mover físicamente el recurso. Adicionalmente, el movimiento de los recursos virtualizados entre la gestión de un elemento de gestión a otro elemento de gestión (por ejemplo, un evento de Movimiento, o migración de una infraestructura virtual a otra) se puede rastrear, como puede la ubicación de los recursos físicos, a través de las conexiones entre el software de control de seguridad y varios componentes de gestión de recursos.

Las modalidades de la presente descripción pueden mover un recurso (es decir, cambiar su membresía de zona lógica) de una Zona de Confianza a otra (430) como se dese. Tal como cuando el nombre VM del atributo de recurso cambia. En otras modalidades, los diferentes atributos o combinaciones de atributos para el recurso, otros recursos, o cualquier elemento se pueden monitorear para cambiar y afectar el mismo comportamiento del cambio de la Zona de Confianza para un recurso. Por consiguiente, como se ilustra en lo anterior, la

póliza del servidor de seguridad se puede mantener o cambiar (en su totalidad o en parte) con base en la naturaleza de los cambios de atributos detectados por las características de implementación del software de control de seguridad de la presente descripción.

Las modalidades de la presente descripción tienen utilidad significativa cuando se consideran los atributos de recursos derivados de la operación de otros controles técnicos de seguridad similares a un scanner de vulnerabilidad o detección de software maligno. Nuevas vulnerabilidades y virus están siendo constantemente descubiertos, de modo que las modalidades de la descripción pueden ayudar a facilitar el pre-planeamiento y pre-configuración de las metas contramedidas para estos eventos al permitir que el arquitecto configure las Zonas de Confianza con más acceso de la red limitada o sin acceso a la red en lo absoluto.

Con referencia nuevamente a la FIGURA 4, en la detección de una vulnerabilidad de seguridad (tal como un virus u otro software maligno, o un defecto en el hardware o software) o en un recurso (425), el software de control de la seguridad de la presente descripción podría limitar automáticamente o terminar el acceso a la red al mover el recurso (430) a una Zona de Confianza predefinida hasta que otro técnico de

seguridad automatizado controle la actualización del software de vulnerabilidad o remueve el virus. Esta cuarentena se podría remover automáticamente en respuesta a la detección de la condición de atributo de recurso que inició el movimiento automatizado del recurso que se elimina (420), o del software de control de seguridad que recibe otra indicación de que la vulnerabilidad de seguridad se ha abordado. Una vez que la vulnerabilidad de seguridad se aborda, el recurso se puede mover automáticamente de nuevo a la Zona de Confianza original y las pólizas de acceso de red originales (como se expresa en ZACL) se restauran automáticamente.

Para varios marcos de conformidad, el software de control de seguridad de la presente descripción puede llevar a cabo un mapeo lógico entre los controles de conformidad en el marco y varios controles técnicos de seguridad (controles técnicos). Los controles administrativos también se pueden mapear a los controles de conformidad en los marcos, a través de (por ejemplo) eventos que son generados por el software de control de seguridad y que indican la terminación de las interacciones del operador específicas con el software de control de seguridad, que indican la terminación de un flujo de trabajo (un proceso o procedimiento que se debe completar), y/o que cumple con el control administrativo como se define en el marco. Este mapeo es referido como un mapeo

de conformidad y, en una modalidad de la descripción, se implementa dentro de los componentes lógicos y heurísticos de póliza y referencia, y la base de datos de la póliza (ver FIGURA 2).

5 Con referencia nuevamente a la FIGURA 1, una o más pólizas de control de conformidad se pueden asociar con una o más zonas lógicas y/o recursos (440). Cuando los controles técnicos requeridos por el control de conformidad se validan como se colocan para un recurso en una zona lógica, el
10 software de control de seguridad, usando el mapeo de conformidad, puede ajustar el nivel de conformidad para el control de conformidad por consiguiente.

 Para los controles técnicos de seguridad, la validación de la aplicación del control técnico de seguridad a cualquier
15 recurso se puede llevar a cabo por el software de control de seguridad de la presente descripción basada en los mecanismos de sonicación lógicos y la membresía en una Zona de Confianza con las pólizas apropiadas para el control de técnico de seguridad como se describe en lo anterior para el servidor de
20 seguridad. Cualquiera de los controles técnicos de seguridad adicionales se puede validar también (por ejemplo IPS, Escáner de Vulnerabilidad, auditoría de flujo), tal como a través de varias interacciones con los elementos de gestión para varios controles técnicos.

Para los controles administrativos, se han completado los eventos de SCMS que indican que una secuencia de las operaciones solicitadas por el operador dentro de la interfaz de usuario del software de control de seguridad, validan que el control administrativo se ha cumplido. Un ejemplo de un control administrativo es la producción e intercambio de reportes. En este ejemplo, el operador programa un reporte y designa una lista de contactos para recibir el reporte. En la terminación del programa, se genera un evento indicando que el reporte se programa para envío, cumpliendo de esta manera con cualquier control administrativo que requiera la colaboración o intercambio de información contenida en cualquier reporte disponible. Las modalidades alternas podrían implementar eventos para cualquier secuencia de interacciones (por ejemplo Configuración Wizards) para cualquier proceso o procedimiento y validar cualquier número de procesos y procedimientos relacionados con la operación y configuración de los controles técnicos de seguridad, controles administrativos, elementos de gestión, elementos de seguridad, elementos de red, y elementos de computación en el entorno de computación, proporcionando de esta manera la validación de los controles de conformidad que son de naturaleza procesal.

Cuando la adherencia a un marco de conformidad

particular es deseable, el operador puede, a través de los componentes de creación y configuración de la zona lógica (ver FIGURA 2), selecciona un marco de conformidad para cualquiera de la Zona de Confianza o Zonas de Confianza. Una vez que un ajuste de marco de conformidad se aplica a una Zona de Confianza, las pólizas y configuraciones de todos los controles de seguridad técnicos y los controles administrativos llevados a cabo se evalúan dentro del contexto del mapeo de conformidad para el marco de conformidad seleccionado.

El software de control de seguridad puede analizar una o más modificaciones a los ajustes de configuración del servidor de seguridad (445). Ya que cada control se configura, el software de control de seguridad, usando el mapeo de conformidad, genera un nivel de conformidad (450) para cada control de conformidad que es soportado por los controles técnicos de seguridad y las secuencias de control administrativas.

Los mapeos de conformidad pueden combinar los controles técnicos validados donde la información de un control técnico o póliza no es suficiente para asegurar la conformidad con los controles de conformidad. Por ejemplo, en el ejemplo anterior, la implementación del servidor de seguridad del control de acceso, el ACL, es solo suficiente para asegurar

que el recurso se proteja por el seguidor de seguridad, cuando la dirección IP del atributo de recurso sigue siendo la misma como la configurada en el ACL del servidor de seguridad. Los ejemplos anteriores muestran que para cualquier recurso, la dirección IP de atributo puede y cambiará. A través de la combinación del control VIM que monitorea los cambios del atributo de recurso para los recursos de información virtualizados (VMs), incluyendo los cambios de la dirección IP de atributo de recurso, el mapeo de conformidad (que combina estos controles para este propósito) de la presente descripción proporciona una afirmación sólida de conformidad, que los métodos convencionales de monitoreo de los ACLs de servidor de seguridad solos. Esta combinación específica del control VIM y el servidor de seguridad se pueden generalizar a cualquier combinación de VIM de cualquier control técnico de seguridad de la red que depende de la dirección IP del atributo de recurso para funcionar correctamente. La combinación de diferentes controles de seguridad técnicos y administrativos se pueden generalizar adicionalmente para mejorar la aserción de los controles de conformidad a través, por ejemplo, del uso de la sonicación lógica que permite la aplicación y validación de varias pólizas de control de seguridad en una manera validada.

Como se describe en lo anterior, las modalidades de la presente descripción pueden actualizar las pólizas para los servidores de seguridad automáticamente en respuesta a los cambios de la dirección IP, manteniendo de esta manera la conformidad. Este escenario ilustra como evaluar varios controles técnicos que algunas veces pueden ser deseables para ayudar a mantener la conformidad con los marcos de conformidad, y muestra las capacidades ventajosas de las modalidades de la presente descripción. Aunque este ejemplo de control técnico de seguridad combinado para el mapeo de conformidad utiliza solo dos controles técnicos de seguridad, el número de controles técnicos de seguridad y/o eventos que se pueden combinar para el mapeo de conformidad no se vinculan, y las combinaciones de los números arbitrarios se pueden utilizar en las modalidades de la presente descripción. En la FIGURA 5, por ejemplo, la gráfica 500 ilustra tres controles técnicos a lo largo del eje x, con el nivel contribuido de conformidad para un control de conformidad a lo largo del eje y.

La aplicación de los controles de servidor de seguridad como se describe en lo anterior se puede validar por la sonicación lógica para cualquier recurso en una Zona de Confianza con un listado de ZACL. Para cualquier control de conformidad que requiera la implementación de los controles

de acceso de base de la red aplicados por un servidor de seguridad, el software de control de seguridad puede utilizar el mapeo de conformidad instanciado en combinación con otros controles técnicos de seguridad validados para calcular el nivel de conformidad actual para cada control de conformidad soportado. Cada control técnico de seguridad en una combinación, como es expresado en el mapeo, puede contribuir a la porción normalizada de una medición de nivel de conformidad definido. Estos niveles pueden ser representados numéricamente, tal como un nivel entre 0 y 3, y ese nivel se muestra gráficamente (455) en tiempo real o en tiempo casi real como se muestra en la FIGURA 7. Los niveles de conformidad (tales como las puntuaciones numéricas) se pueden generar para cualquier número de zonas lógicas, recursos, u otros componentes de hardware y software (tal como el servidor de seguridad) y se pueden evaluar simultáneamente contra varios marcos de conformidad a través de mapeos de conformidad alternos.

Los marcos de conformidad se configuran en general para proteger los datos, tales como los datos del titular de la tarjeta en el caso de la norma de seguridad de datos Industriales de Tarjeta de Pago (PCI). En general, el número de elementos individuales en el entorno de computación que procesa los datos sometidos a cualquier marco de conformidad

es mayor que uno y es típicamente muchos. La suma total de todos los elementos o recursos que procesan los datos que se someten a un marco de conformidad es referida como el alcance de conformidad. El nivel de conformidad del entorno de computación, relevante a cualquier marco, puede solo ser tan alto como el nivel medido en el último recurso de conformidad dentro del alcance de conformidad. La sonicación lógica soporta la inclusión de varios recursos de información en cualquier zona de confianza. Para cualquier Zona de Confianza con un conjunto de marcos de conformidad, el software de control de seguridad mide el nivel de conformidad para todos los controles de conformidad soportados, para cada recurso dentro de la zona de confianza. El nivel de Zona de Confianza agregado de conformidad como es visualizado por cualquier control de conformidad se calcula como el nivel de conformidad medido más bajo para todos los recursos dentro de la zona de confianza.

Las FIGURAS 6 y 7 ilustran como una modalidad ejemplar de la presente descripción, que usa un formato de gráfica radial, muestra el nivel de conformidad para varios controles de conformidad (455). En este ejemplo, la gráfica muestra la conformidad para el marco PCI DSS 2.0, pero los niveles de conformidad pueden ser representados gráficamente para cualquier variedad de normas de conformidad diferentes en la

misma o diferentes gráficas.

Con la gráfica radial 700 en la FIGURA 7, el nivel de conformidad agregado para todos los controles de conformidad se muestra para todos los recursos en una Zona de Confianza llamado "Pago" con base en los métodos de cálculo descrito en lo anterior. Para cada control de conformidad, el nivel de conformidad calculado se muestra como un elemento radial de la gráfica radial y se identifica con el número de sección del marco de conformidad.

Las modalidades de la presente descripción pueden contener varios mapeos de conformidad por los cuales los niveles de conformidad para cada Zona de Confianza se calculan y se muestran basados en el conjunto de marcos de conformidad específicos y únicos para esa zona de confianza. Por ejemplo, un entorno de computación puede contener datos que se someten a varios marcos de conformidad. Entre otras cosas, la sonicación lógica con las Zonas de Confianza permite el agrupamiento de recursos basados en estos marcos de conformidad y el reporte de los niveles de conformidad para esos marcos específicos y distintos simultáneamente, incluyendo la capacidad de medir los niveles de conformidad para un recurso dentro del contexto de varios marcos de conformidad a través del proceso de agregar ese recurso a varias Zonas de Confianza con diferentes ajustes de marcos de

conformidad.

La FIGURA 8 muestra un diagrama de bloque del sistema que se puede usar en conjunción con varias modalidades. Aunque la FIGURA 8 ilustra varios componentes de un sistema de computadora, no se propone para representar ninguna arquitectura particular o manera de interconectar los componentes. Otros sistemas que tienen menos o más componentes también se pueden usar.

En la FIGURA 8, el sistema 800 incluye un sistema de computadora anfitrión 810 que comprende un procesador 812, memoria 814, e interfaz de usuario 816. El sistema de computadora anfitrión 810 puede incluir cualquier número de procesadores diferentes, componentes de memoria, y componentes de interfaz de usuario, y puede interactuar con cualquiera de otro sistema deseado y dispositivos en conjunción con las modalidades de la presente descripción.

La funcionalidad del sistema anfitrión 810, que incluye los métodos representados en las FIGURAS 4 y 9, (en totalidad o en parte), se puede implementar a través del procesador 812 que ejecuta instrucciones legibles por computadora almacenadas en la memoria 814 del sistema 810. La memoria 814 puede almacenar cualquiera de las instrucciones legibles por computadora y datos, incluyendo aplicaciones de software y código de operación incorporado.

La funcionalidad del sistema anfitrión 810 u otro sistema y dispositivos que funcionan en conjunción con las modalidades de la presente descripción también se pueden implementar a través de varios componentes de hardware que

5 almacenan instrucciones legibles por máquina, tal como circuitos integrados específicos de aplicación (ASICs), arreglos de compuerta programables en campo (FPGAs) y/o dispositivos lógicos programables complejos (CPLDs). Los sistemas de acuerdo con los aspectos de ciertas modalidades

10 pueden funcionar en conjunción con cualquier combinación deseada de componentes de software y/o hardware. El procesador 812 recupera ejecuta las instrucciones almacenadas en la memoria 814 para controlar la operación del sistema 810. Cualquier tipo de procesador, tal como un

15 microprocesador de circuito integrado, microcontrolador, y/o procesador de señal digital (DSP), se pueden usar en conjunción con las modalidades de la presente descripción. Una memoria 814 que opera en conjunción con las modalidades de la descripción puede incluir cualquier combinación de

20 diferentes dispositivos de almacenamiento de memoria, tales como discos duros, memoria de acceso aleatorio (RAM), memoria sólo de lectura (ROM), memoria FLASH, o cualquier otro tipo de memoria volátil y/o no volátil. Los datos se pueden almacenar en la memoria 814 de cualquier manera deseada.

El sistema anfitrión 810 incluye una interfaz de usuario 816 que puede incluir cualquier número de dispositivos de entrada (no mostrados) para recibir comandos, datos, y otra entrada adecuada de un usuario, así como cualquier número de dispositivos de salida (no mostrados) para proporcionar al usuario con datos, notificaciones, y otra información adecuada. Los dispositivos I/O típicos pueden incluir ratones, teclados, módems, interfases de red, impresoras, escáneres, cámaras de video y otros dispositivos.

El sistema anfitrión 810 puede comunicarse con uno o más dispositivos del cliente 820 y otros sistemas y dispositivos en cualquier manera deseada, incluyendo a través de la red 830. El dispositivo de cliente 820 puede incluir cualquier dispositivo de computadora que funcione en conjunción con los sistemas y métodos de la presente descripción. El dispositivo de cliente 820 puede ser, o incluir, una computadora portátil, una computadora de escritorio, un dispositivo de comunicación de subscritor móvil, un teléfono móvil, un asistente digital personal (PDA), una computadora tableta, un libreo electrónico o lector de libros, una cámara digital, una cámara de video, una consola de juegos de video y/o cualquier otro dispositivo de computación adecuado.

La red 8300 puede incluir cualquier sistema o método de comunicaciones electrónicas. La comunicación entre los

componentes que funcionan en conjunción con las modalidades de la presente descripción se puede llevar a cabo usando cualquier método de comunicación adecuado, tal como, por ejemplo, una red telefónica, un extranet, un intranet, el Internet, punto de dispositivo de interacción (punto de dispositivo de venta, asistente digital personal (por ejemplo, iPhone^{MR}, Palm Pilot^{MR}, Blackberry^{MR}), teléfono celular, kiosco, etc.), comunicaciones en línea, comunicaciones satelitales, comunicaciones fuera de línea, comunicaciones inalámbricas, comunicaciones de transpondedor, red de área local (LAN), red de área ancha (WAN), red privada virtual (VPN), dispositivos conectados a la red o ligados, teclado, ratón y/o cualquier modalidad de entrada de comunicación o datos adecuada. Los sistemas y dispositivos de la presente descripción pueden utilizar protocolos de comunicaciones TCP/IP así como IPX, Appletalk, IP-6, NetBIOS, OSI, cualquier protocolo de tunelización (por ejemplo IPsec, SSH), o cualquier número de protocolos existentes o futuros.

Sistemas Métodos para Análisis y Reporte de Flujo de la Red

Muchos sistemas convencionales para el monitoreo de la red, control de la red, y seguridad de la red usan típicamente datos de flujo de la red de enrutadores, conmutadores, u otro hardware configurado para recolectar estadísticas de tráfico de la red usando una norma conocida como "Exportación de

Información de Flujo IP" (IPFIX), que también es conocida como "Netflow". El IPFIX permite el monitoreo (por ejemplo, auditoría) de los intercambios de la red entre los recursos y, algún grado, califica los intercambios de información basados en los atributos de conexión de la red, tal como dirección IP, números de puerto de fuente y destino, así como conteo de bits y otros atributos de paquete o conexión definidos en el protocolo IPFIX e implementados por el dispositivo de envío IPFIX o software. Sin embargo, los sistemas convencionales no pueden ser capaces de contextualizar las conexiones de la red representadas con IPFIX con los datos de otras fuentes, tales como los datos de un sistema de detección de intrusión, sistema de prevención de intrusión (IDS), datos de escaneo de vulnerabilidad (IPS), datos de configuración, datos de anti-virus/anti-software maligno, pólizas aplicadas a los controles técnicos de seguridad, datos de configuración del sistema operativo, datos de configuración de la aplicación, procesos que se ejecutan en el recurso (procesos del sistema de aplicación u operación), identificación de usuario que inicia el proceso, firmas digitales binarias y/o datos de los servidores de seguridad.

Adicionalmente, los sistemas convencionales no pueden ser capaces de correlacionar y proporcionar contextos y

relaciones causales y resultantes entre estos elementos de datos y las acciones llevadas a cabo en el entorno de computación por sus componentes generadores de perspectiva. Las modalidades de la presente descripción, en contraste, pueden recolectar y analizar datos de recurso y de la red de las diversas fuentes, y usar estos datos para presentar una representación más completa y precisa de la postura de seguridad y los fenómenos relevantes de seguridad comparados con los sistemas convencionales tal, por ejemplo, soportar y al llevar a cabo los análisis de combinación complejos para la correlación de eventos, conexiones de la red, estados operacionales de recurso, y los estados de los controles técnicos de seguridad.

La FIGURA 9 representa un proceso ejemplar de acuerdo con varias modalidades de la presente descripción. Cualquier combinación y/o subconjunto de los elementos del método en la FIGURA 9 se pueden practicar en cualquier orden adecuado y en conjunción con cualquier sistema adecuado, dispositivo, y/o proceso, incluyendo el proceso mostrado en la FIGURA 4 y el sistema mostrado en la FIGURA 8. En la FIGURA 9, el método incluye recolectar datos (por ejemplo, datos de recurso y/o de la red) de diferentes fuentes (905), filtrar los datos (910), identificar uno o más eventos y recursos asociados con estos eventos de los datos (915), identificar conexiones

entre los recursos y características de los mismos de los datos (920), y generar (925) y presentar (930) una gráfica de información de flujo. El método 900 incluye además recibir una selección de un componente en la gráfica de información de flujo (935), mostrar la información adicional en respuesta a la selección (940), recibir ediciones a las reglas de tráfico a la red (945) y aplicar estas reglas a la red (950). El método 900 incluye adicionalmente recolectar datos actualizados (955) y actualizar la gráfica de información de flujo con los datos actualizados (960). El método 900 también incluye almacenar datos (965), analizar los datos (970), generar una o más alertas (975), generar uno o más reportes (980), y exportar los datos (985).

Las modalidades de la presente descripción pueden recolectar datos (905) de cualquier número de diferentes fuentes y/o diferentes tipos de fuentes, incluyendo los datos con respecto al recurso, eventos de la red, y atributos de operación del sistema. Estos datos recolectados pueden incluir, por ejemplo, atributos de flujo de la red, información de un usuario de un recurso, información con respecto a un recurso así como componentes de hardware y/o virtuales asociados con un recurso, información en las aplicaciones de software, atributos de diferentes nodos de la red, vulnerabilidades de seguridad, atributos de una red de

recursos, información en el contenido de los paquetes de datos, así como cualquier otra información deseada. En un ejemplo, un métodos que implementa el sistema 900 se puede recolectar datos de flujo de la red (por ejemplo, información
5 que se refiere a intercambios de mensajes e intercambios de mensajes intentados) entre los recursos virtuales y físicos en una red de componentes de hardware (tales como enrutadores y conmutadores o sus análogos virtuales) que recolectan datos "Netflow". Adicionalmente o alternativamente, los datos se
10 pueden recolectar de una o más de otras fuentes, tal como un sistema de detección de intrusión (IDS), un sistema de prevención de intrusión (IPS), y/o un servidor de seguridad. Los datos que se recolectan también pueden incluir atributos o pólizas de configuración de control técnicos de seguridad
15 que definen el tráfico permitido y bloqueado entre los recursos específicos, grupos de recursos, y/o zonas lógicas. En algunas modalidades, una lista de tráfico permitido y bloqueado se puede definir para variaciones lógicas, y se puede referir en la presente como una "lista de control de
20 acceso de zona" (ZACL).

Los datos pueden recibirse o recolectar (905) en cualquier manera adecuada, tal como acumular y/o al recibir las corrientes de datos (como en las corrientes IPFIX, registros de sistema, APIs, etc.). Los datos se pueden

recolectar de varias fuentes, normalizadas y combinadas en una lista de registros para propósito de asociar todos los "atributos" con los datos de flujo de la red, permitiendo de esta manera que las modalidades de la descripción creen y
5 presentes correlaciones en varios métodos incluyendo gráficas como se describe en la presente adicionalmente.

Los datos recolectados de diferentes fuentes se pueden filtrar (910) en una variedad de formas. Por ejemplo, los datos de diferentes fuentes se pueden usar para poblar una
10 estructura de datos, con los datos que son redundantes a los datos de otra fuente removida para producir de esta manera una estructura de datos con atributos de flujo de la red únicos y características recolectadas de las diferentes fuentes. Los datos de vulnerabilidad recibidos de un escaneo
15 se pueden asociar (por ejemplo, a través de los procesos de normalización y correlación descritos en la presente) con un flujo de red específico, permitiendo de esta manera que el usuario de un sistema identifique las relaciones entre los diversos estados operacionales del recurso y conexiones de la
20 red de o al recurso o a una pluralidad de recursos. Los datos recolectados también se pueden filtrar de acuerdo con la preferencia del usuario. Por ejemplo, el usuario se puede interesar en un evento de la red particular (tal como una violación de seguridad) y de esta manera el sistema que

implementa el método 900 puede filtrar automáticamente (o en respuesta a la entrada de usuario específica) datos no relacionados a un recurso violado específico o servicio de aplicación y comprometido que se ejecuta en uno o más
5 recursos.

Las modalidades de la presente solicitud pueden identificar varios eventos de tráfico de la red, y los recursos de la red relacionados con esos eventos, basados en los datos recolectados (910). Un evento puede incluir, por
10 ejemplo, un intercambio de paquetes de datos entre dos recursos en una red, una violación de seguridad intentada actual, una actualización de software, un fallo (por ejemplo, hardware y/o software) asociado con un recurso, así como otros eventos. Un evento se puede definir sobre uno o más
15 períodos de tiempo, y las modalidades de la presente descripción pueden operar en los datos recibidos en tiempo real (o casi en tiempo real) o en los datos previamente registrados y almacenados. Por ejemplo, un usuario de una red financiera puede desear revisar el tráfico de la red entre
20 cuatro recursos de la red específicos registrados sobre un período de tres horas para investigar un posible intento de fraude electrónico. En este ejemplo, un sistema que implementa la presente descripción puede recuperar los datos de la red para el período de tiempo definido, filtrar los

datos no relacionados a los cuatro recursos o la ventana de tres horas, e identificar automáticamente los eventos y recursos asociados con fraude potencial.

Las modalidades de la presente descripción del mismo modo son capaces de identificar varias conexiones entre los recursos (920), así como las características de estas conexiones y recursos. Por ejemplo, los datos recolectados por el sistema (905) se pueden usar para identificar: datos con respecto a uno o más recursos, datos con respecto a uno o más eventos de la red, y/o datos con respecto a uno o más tributos operacionales del sistema. Las características de los recursos y/o las conexiones entre los recursos se pueden definir o limitar con base en la filtración de los datos recolectados (910). Las características de las conexiones entre los recursos pueden incluir, por ejemplo, el tamaño de los datos comunicados, tiempos cuando los datos se comunican, la fuente(s) y el destino(s) de los datos, la velocidad en la cual los datos se comunican, y otras características.

En el método ejemplar 900, se genera una gráfica de información de flujo (925) para mostrar visualmente varios recursos de la red y conexiones entre estos recursos. La gráfica de información de flujo después se presenta (930) a un usuario, tal como a través de una pantalla de interfaz de usuario de un dispositivo de cliente operado por el usuario

(por ejemplo, dispositivo de cliente 820 en la FIGURA 8). La FIGURA 10 ilustra un ejemplo de una gráfica de información de flujo. En este ejemplo, el tráfico de la red entre varios recursos de la Zona de Confianza se muestra a través de las líneas de flujo direccionales seleccionables. La gráfica de información de flujo representa el tráfico de la red que se permite entre los recursos de la red (es decir, a través de las líneas de flujo sólidas) y el tráfico que se bloquea (es decir, a través de las líneas de flujo punteadas).
Adicionalmente, cada línea de flujo se etiqueta para indicar el tipo de la fuente de los datos usados para identificar la conexión (es decir, "Netflow," "Flujo IDS", "Flujo IPS", "ZACL Permitido", y "ZACL Negado").

Una selección de un componente (por ejemplo, un recurso de la red o conexión entre los recursos) se puede recibir (935) de un usuario. Por ejemplo, en un caso donde la gráfica de información de flujo se presenta en la pantalla de visualización del dispositivo de cliente 820 controlada por un usuario, el usuario puede seleccionar (por ejemplo, usando un ratón) un línea de flujo para llevar a cabo varias acciones. Por ejemplo, la selección de la línea de flujo puede mostrar la información adicional asociada con la conexión (940), tal como al presentar al usuario con características (por ejemplo, identificadas en el paso 920)

de la conexión asociada con la línea de flujo. La selección de la línea de flujo también puede permitir que el usuario observe y edite (945) las reglas para permitir y bloquear el tráfico sobre la conexión. Las reglas editadas de esta manera
5 después se pueden aplicar a la conexión (950).

La gráfica de la información de flujo puede ser representada en conjunción con la información de flujo de la red, reglas, y otros datos, en un formato de tabla, un ejemplo del cual se representa en la FIGURA 11. Entre otras
10 cosas, la tabla en la FIGURA 11 permite que un usuario busque y/o filtre los datos en la tabla usando diferentes campos (tal como con base en la marca de tiempo, nombre del recurso de origen, u otro atributo) y crear y editar las reglas al, por ejemplo, hacer doble clic a una entrada en la tabla.

15 La FIGURA 12 ilustra una captura de pantalla ejemplar que muestra un campo de descripción de la regla ZACL que puede ser presentada en una tabla de datos (tal como la tabla de datos en la FIGURA 11) así como en respuesta a la selección de un componente en la gráfica de la información de
20 flujo por un usuario. Como se muestra, el “diálogo de entrada del campo de descripción” se puede usar para un usuario para editar una regla que se aplica a una conexión entre recursos.

La FIGURA 13 ilustra otra captura de pantalla ejemplar que muestra las reglas ZACL que son accionadas. En este

ejemplo, los eventos donde el tráfico se permite por una regla de ZACL provocan que la regla se destaque en verde, mientras que los eventos donde el tráfico se bloquea provocan que la regla de ZACL se destaque en rojo. Otros indicadores
5 visuales para mostrar el tráfico permitido/bloqueado también se pueden usar.

Las FIGURAS 14 y 15 ilustran la creación de objetos de la red (FIGURA 14) y el uso del objeto de la red en las reglas ZACL (FIGURA 15). La FIGURA 16 ilustra una regla ZACL
10 que tiene varias fuentes y destinos.

La FIGURA 17 ilustra el tráfico bloqueado y permitido a través de las líneas sólidas y punteadas (respectivamente) en la gráfica de información de flujo, así como un menú desplegable en una tabla de datos asociada con la gráfica de
15 la información de flujo que permite que el usuario seleccione "acceder a ZACL". La selección o des-selección del acceso con una regla de ZACL permite que un usuario incluya o remueva (respectivamente) los aciertos de la regla, de la regla en la gráfica de información de flujo.

20 La FIGURA 18 ilustra una característica de "flujos de purga" de una modalidad ejemplar, mediante el cual los flujos específicos se pueden seleccionar y remover de la gráfica de información de flujo, permitiendo de esta manera que un usuario se enfoque con más precisión en un conjunto deseado

de conexiones.

La FIGURA 19 ilustra la filtración de los flujos antes de que se muestre en la gráfica de información de flujo (FIGURA 10) o la tabla de datos (FIGURA 11). Esto ayuda
5 adicionalmente a un usuario a seleccionar los flujos específicos de interés para el usuario.

Como se describe en lo anterior, la gráfica de información de flujo puede representar una variedad de diferentes recursos de la red con respecto a la información y
10 las condiciones de la red entre estos recursos. Las FIGURAS 20-22 ilustran ejemplos de gráficas de información de flujo que identifican las características de conexiones entre los recursos de la red y/o características de los recursos. La identificación de estas características puede presentarse en
15 respuesta a la selección de un atributo u otra entrada de usuario de un usuario a través de un interfaz de usuario y/o pasará en la selección automática de las características por los sistemas que implementan las modalidades de la presente descripción.

20 La FIGURA 20 ilustra un gráfica de información de flujo ejemplar donde un usuario ha seleccionado "datos de flujo" de entre una lista de atributos de un conjunto de datos recolectados. En este ejemplo, el icono de "datos de flujo" a la izquierda de la pantalla se destaca, y las líneas de flujo

en negritas se dibujan entre cada una de los cinco recursos de la red (es decir, las Zonas de Confianza en este ejemplo) para mostrar su conectividad respectiva basada en los atributos de "datos de flujo" seleccionados. Además de poner
5 en negritas y destacar, las características de los recursos y las conexiones de la red se pueden indicar visualmente en una gráfica de información de flujo usando varias combinaciones de textos, puentes, iconos, sombreados y similares.

Cualquier variedad de diferentes atributos se pueden
10 usar para representar visualmente las conexiones de la red con respecto a la información y recursos en una gráfica de información de flujo. En la FIGURA 21, por ejemplo, una vulnerabilidad particular del menú de "datos de vulnerabilidad" a la izquierda de la pantalla se selecciona.
15 En este punto, el sistema ha identificado un recurso en la gráfica de información de flujo (es decir, el recurso "TrustZone PCI App1 Web") por ser asociado con la vulnerabilidad (por ejemplo, que tiene la vulnerabilidad debido a software desactualizado) que se destaca.
20 Adicionalmente, un identificador de usuario ("bobjones") del menú de tributos de "datos de la máquina" también se selecciona, y la conexión entre el recurso de "Usuarios de TrustZone PCI App1" y el recurso "TrustZone PCI App1 Web" se identificar por el sistema por ser asociado con el

identificador de usuario seleccionado y destacado en la gráfica de información de flujo por consiguiente. La FIGURA 22 representa la apariencia de la gráfica de la información de flujo en respuesta a la des-selección del atributo de

5 "datos de la máquina" de la FIGURA 21, dejando solo el recurso de "TrustZone PCI App1 Web" destacado para corresponder con la vulnerabilidad de seguridad seleccionada.

Las FIGURAS 23 y 24 representan ejemplos adicionales de información que se pueden representar por las gráficas de

10 información de flujo. En la FIGURA 23, tanto los atributos de "datos de vulnerabilidad" y "datos de flujo" se seleccionan, como se muestra por su destacado respectivo. En la parte superior de la gráfica, la información en los tres recursos en la red se muestra, mientras que la gráfica muestra los

15 datos de la red asociados con los recursos en la forma de datos de flujo "entrantes" a la izquierda de la gráfica y los datos de flujo "de salida" a la derecha de la gráfica. Los atributos operacionales del sistema se muestran adicionalmente en la mitad de la gráfica. La FIGURA 24

20 ilustra la gráfica de información de flujo de la FIGURA 23 sin el atributo de "datos de flujo" que se seleccionan.

Los datos actualizados se pueden recolectar (955) sobre una base periódica o en tiempo real/casi en tiempo real. La gráfica de la información de flujo mostrada a un usuario del

mismo modo se puede actualizar y presentar para mostrar cambios para los recursos y/o conexiones sobre una base periódica o en tiempo real/casi en tiempo real.

Las modalidades de la solicitud pueden almacenar (965) y
5 analizar (970) los datos recolectados, con datos relacionados con la generación y/o presentación de la gráfica de información de flujo, y otra información. Por ejemplo, el sistema que implementa el método 900 puede almacenar los datos recolectados y usarlos para generar una gráfica de
10 información de flujo, así como una captura de pantalla de una gráfica de información de flujo particular en un punto de tiempo particular durante un período de tiempo particular, permitiendo de esta manera que un usuario recupere una gráfica deseada sin tener que recrearla desde cero.
15 Cualquiera de los datos deseados se puede analizar para una variedad de propósitos. Por ejemplo, los datos recolectados se pueden analizar (por ejemplo, comparándola a una póliza de seguridad, las normas de la póliza de conformidad y/o una norma de desempeño) y generar una o más alertas (975) basadas
20 en el análisis.

También se pueden generar varios reportes (980) y presentar a los usuarios del sistema y/o terceros. Un reporte se puede incluir en un documento electrónico, y puede proporcionar un resumen del estado, estado, y/o historial de

algún aspecto de una red, Zonas de Confianza, y/o recursos individuales. En una modalidad ejemplar, se puede crear un reporte que detalla el estado de conformidad de todos los recursos en la Zona de Confianza en el momento que el reporte se ejecuta. En otro ejemplo, un reporte se puede crear para detallar las vulnerabilidades detectadas de todos los recursos en una Zona de Confianza o un recurso particular. Los reportes también se pueden generar para proporcionar un resumen de la información en un punto particular en el tiempo (por ejemplo, una “captura de pantalla”) o un resumen de la información durante un período de tiempo (por ejemplo, que muestra tendencia en los datos) para las Zonas de Confianza y/o recursos. Las modalidades ejemplares también pueden generar un reporte que detalla la Lista de Control de Acceso de Zona (ZACL), y todos los recursos con su dirección(es) IP de recursos y la membresía de la Zona de Confianza.

El método 900 incluye además exportar la información (985) a terceros. Cualquiera de esta información se puede exportar, tal como los datos recolectados, la gráfica de información de flujo, y otra información, permitiendo de esta manera que los terceros lleven a cabo su propio análisis y procesamiento de estos datos. Los datos se pueden exportar a terceros de cualquier manera deseada, tal como a través de una interfaz de programa de aplicación (API), a través de una

corriente de datos en tiempo real o casi en tiempo real, o a través de cualquier otra interfaz deseada.

La funcionalidad de varias modalidades se puede llevar a cabo a través de un buscador de la red y/o aplicación que interactúa utilizando un buscador de la red. Tales aplicaciones del buscador pueden comprender software buscador de Internet instalado dentro de una unidad de computación o un sistema para llevar a cabo varias funciones. Estas unidades de computación o sistemas pueden tomar la forma de una computadora o conjunto de computadoras, y cualquier tipo de dispositivo o sistema de computación se pueden usar, incluyendo computadoras portátiles, minicomputadoras, tabletas, computadoras portátiles, asistentes digitales personales, decodificadores, estaciones de trabajo, servidores de computadora, computadoras de marco principal, minicomputadoras, servidores de PC, computadoras ubicuas, conjuntos de red de las computadoras, computadoras personales y computadoras de tableta, tales como iPads, iMACs, y MacBooks, quioscos, terminales, dispositivos de punto de venta (POS) y/o terminales, televisiones, o cualquier otro dispositivo capaz de recibir datos sobre una red. Varias modalidades pueden utilizar Microsoft Internet Explorer, Mozilla Firefox, Google Chrome, Apple Safari, o cualquier otro de infinidad de paquetes de software disponibles para

buscar en el internet.

Varias modalidades pueden operar en conjunción con cualquier sistema operativo adecuado (por ejemplo, Windows NT, 95/98/2000/CE/Mobile, OS2, UNIX, Linux, Solaris, MacOS, 5 PalmOS, etc.) así como varios software y controladores de soporte convencionales asociados típicamente con las computadoras. Varias modalidades pueden incluir cualquier computadora personal adecuada, computadora de red, estación de trabajo, asistente digital personal, teléfono celular, 10 teléfono inteligente, minicomputadora, mini-estructura y similares. Las modalidades pueden implementar protocolos de seguridad, tales como Capa de Conexiones Seguras (SSL), Seguridad de Capa de Transporte (TLS), y Cubierta Segura (SSH). Las modalidades pueden implementar cualquier protocolo 15 de capa de aplicación deseada, incluyendo http, https, ftp, y sftp.

Varios componentes, módulos, y/o motores se pueden implementar como micro-aplicaciones o micro-apps. Las micro-apps se despegan típicamente en el contexto de un sistema 20 operativo móvil, incluyendo por ejemplo un sistema operativo móvil Palm, un sistema operativo móvil Windows, un Sistema Operativo Android, Apple iOS, un sistema operativo Blackberry y similares. La micro-app se puede configurar para aprovechar los recursos del sistema operativo más grande y hardware

asociado a través de un conjunto de reglas predeterminadas que controlan las operaciones de varios sistemas operativos y los recursos de hardware. Por ejemplo, donde una micro-app se desea comunicar con un dispositivo o red diferente al dispositivo móvil o sistema operativo móvil, la micro-app puede aprovecharse del protocolo de comunicación del sistema operativo y hardware del dispositivo asociado bajo las reglas predeterminadas del sistema operativo móvil. Por otra parte, donde la micro-app desea una entrada de un usuario, la micro-app se puede configurar para solicitar una respuesta del sistema operativo que monitorea varios componentes de hardware y después se comunica con una entrada detectada del hardware a la micro-app.

Como se usa en la presente, el término “red” incluye cualquier nube, sistema de computación en la nube o sistema de comunicaciones electrónico o método que incorpora componentes de hardware y/o software. La comunicación entre las partes se puede lograr a través de cualquiera de los canales de comunicación adecuados, tales como, por ejemplo, una red telefónica, un extranet, un intranet, el Internet, punto de dispositivo de interacción (dispositivo de punto de venta, asistente digital personal (por ejemplo, iPhone^{MR}, Palm Pilot^{MR}, Blackberry^{MR}), teléfono celular, quiosco, etc.), comunicaciones en línea, comunicaciones satelitales,

comunicaciones fuera de línea, comunicaciones inalámbricas, comunicaciones de transpondedor, red de área local (LAN), red de área ancha (WAN), red privada virtual (VPN), dispositivos conectados a la red o ligados, teclado, ratón y/o cualquier
5 otra comunicación adecuada o modalidad de entrada de datos. Los sistemas pueden utilizar protocolos de comunicaciones TCP/IP así como IPX, Appletalk, IP-6, NetBIOS, OSI, cualquier protocolo de tunelización (por ejemplo IPsec, SSH), o cualquier número de protocolos existentes o futuros. La
10 información específica relacionada con los protocolos, normas, y software de aplicación utilizados en relación con el Internet son generalmente conocidos por aquellas personas expertas en la técnica y, como tal, no necesitan ser detallados en la presente.

15 Los diversos componentes del sistema se pueden acoplar independiente, separada o colectivamente de manera adecuada a la red a través de los enlaces de datos que incluyen, por ejemplo, una conexión a un Proveedor de Servicio de Internet (ISP) sobre el bucle local como se usa típicamente en
20 conexión con la comunicación del modem estándar, modem de cable, redes satelitales, ISDN, Línea de Subscritor Digital (DSL), o varios métodos de comunicación inalámbrica. Cabe destacar que la red se puede implementar como otros tipos de redes, tal como una red de televisión interactiva (ITV).

El sistema se puede implementar parcial o completamente usando la computación de la nube. "Nube" o "Computación de la nube" incluyen un modelo para permitir el acceso a la red a petición, conveniente a una acumulación compartida de recursos de computación configurables (por ejemplo, redes, servidores, almacenamiento, aplicaciones, y servicios) que se pueden provisionar rápidamente y liberar con esfuerzo de gestión mínimo o interacción de proveedor de servicio. La computación en la nube puede incluir computación independiente de ubicación, mediante el cual los servidores compartidos proporcionan recursos, software y datos a las computadoras y otros dispositivos a petición.

Varias modalidades se pueden usar en conjunción con los servicios de la red, computación de utilidad, computación ubicua e individualizada, soluciones de seguridad e identidad, computación autonómica, computación en la nube, computación de comodidad, soluciones de movilidad e inalámbricas, fuente abierta, biométrica, computación de la red y/o computación de malla.

Cualquiera de las bases de datos planteadas en la presente puede incluir estructura relacional, jerárquica, gráfica, u orientada al objetivo y/o cualquiera de otras configuraciones de base de datos. Por otra parte, las bases de datos se pueden organizar de cualquier manera adecuada,

por ejemplo, como tabla de datos o tablas de revisión. Cada registro puede ser un archivo individual, una serie de archivos, una serie ligada de archivos de datos o cualquier otra estructura de datos. La asociación de ciertos datos se puede lograr a través de cualquier técnica de asociación de datos deseada tales como aquellas conocidas o practicadas en la técnica. Por ejemplo, la asociación se puede lograr ya sea manual o automáticamente.

Cualquiera de las bases de datos, sistemas, dispositivos, servidores u otros componentes del sistema pueden consistir de cualquier combinación de los mismos en una ubicación individual o en varias ubicaciones, en donde cada base de datos o sistema incluye cualquiera de las diversas características de seguridad adecuadas, tales como servidores de seguridad, códigos de acceso, encriptación, desenscriptación, compresión, descompresión, y/o similares.

La encriptación se puede llevar a cabo por medio de cualquiera de las técnicas ahora disponibles en el campo o que pueden llegar a ser disponibles - por ejemplo, Twofish, RSA, El Gamal, firma Schorr, DSA, PGP, PKI, y criptosistemas simétricos y asimétricos.

Las modalidades pueden contener el Internet o un intranet usando la marcación estándar, cable, DSL o cualquier otro protocolo de Internet conocido en la técnica. Las

transacciones pueden pasar a través de un servidor de seguridad a fin de impedir el acceso no autorizado de usuarios de otras redes.

Las computadoras planteadas en la presente pueden
5 proporcionar un sitio de una red adecuado u otra interfaz de usuario gráfica basada en Internet que sea accesible por los usuarios. Por ejemplo, el Servidor de Información de Internet Microsoft (IIS), Servidor de Transacción Microsoft (MTS), y Servidor Microsoft SQL, se pueden usar en conjunción con el
10 sistema operativo de Microsoft, el software del servidor de la red Microsoft NT, un sistema de base de datos del Servidor Microsoft SQL, y el Servidor de Comercio de Microsoft. Adicionalmente, los componentes tales como Access o el Servidor Microsoft SQL, Oracle, Sybase, Informix MySQL,
15 Interbase, etc., se pueden usar para proporcionar un sistema de gestión de bases de datos de conformidad del Objeto de Datos Activo (ADO). En otro ejemplo, un servidor de la red Apache se puede usar en conjunción con un sistema operativo Linux, una base de datos MySQL, y el Perl, PHP, y/o lenguajes
20 de programación Python.

Cualquiera de las comunicaciones, entradas, almacenamiento, bases de datos, o pantallas planteadas en la presente se pueden facilitar a través de un sitio de la red que tiene páginas de la red. El término "página de la red"

como se usa en la presente no se propone para limitar el tipo de documentos y aplicaciones que se pueden usar para interactuar con el usuario. Por ejemplo, un sitio de la red típico podría incluir, además de los documentos HTML estándares, varias formas, Java applets, JavaScript, páginas de servidores activos (ASP), comandos de interfaz de compuerta comunes (CGI), lenguaje de marcador extensible (XML), HTML dinámico, hojas de estilo de cascada (CSS), AJAX (Asynchronous Javascript And XML), aplicaciones auxiliares, complementos y similares. Un servidor puede incluir un servicio de la red que recibe una solicitud de un servidor de la red, la solicitud incluye la URL y una dirección IP. El servidor de la red recupera las páginas de la red apropiadas y enviar los datos o aplicaciones para las páginas de la red a la dirección IP. Los servicios de la red son aplicaciones que son capaces de interactuar con otras aplicaciones sobre un medio de comunicaciones, tal como el Internet.

Se pueden emplear varias modalidades en cualquier número deseado de métodos para mostrar los datos dentro de un documento con base en el buscador. Por ejemplo, los datos pueden ser representados como texto estándar o dentro de una lista fija, lista deslizable, lista desplegable, campo de texto que se puede editable, campo de texto fijo, ventana emergente, similares. Del mismo modo, las modalidades pueden

utilizar cualquier número deseado de métodos para modificar los datos en una página de la red tales como, por ejemplo, entrada de texto libre usando un teclado, selección de artículos del menú, casillas de verificación, casillas de
5 opción y similares.

Los sistemas y métodos ejemplares ilustrados en la presente se pueden describir en términos de componentes de bloques funcionales, capturas de pantalla, selecciones opcionales y varios pasos de procesamiento. Se debe apreciar
10 que estos bloqueos funcionales pueden llevarse a cabo por cualquier número de componentes de hardware y/o software configurados para llevar a cabo las funciones especificadas. Por ejemplo, el sistema puede emplear varios componentes de circuito integrados, por ejemplo, elementos de memoria,
15 elementos de procesamiento, elementos lógicos, tablas de revisión, y similares, que pueden llevar a cabo una variedad de funciones bajo el control de uno o más microprocesadores u otros dispositivos de control. Similarmente, los elementos de software del sistema se pueden implementar con cualquier
20 lenguaje de programación o scripting tales como C, C++, C#, Java, JavaScript, VBScript, Macromedia Cold Fusion, COBOL, Páginas de Servidor Activo de Microsoft, ensamblaje, PERL, PHP, awk, Python, Visual Basic, Procedimientos Almacenados SQL, PL/SQL, cualquier comando de cubierta UNIX, y lenguaje

de marcación extensible (XML) con los diversos algoritmos que se implementan con cualquier combinación de las estructuras de datos, objetos, procesos, rutinas u otros elementos de programación. Además, cabe destacar que el sistema puede
5 emplear cualquier número de técnicas convencionales para la transmisión de datos, señalización, procesamiento de datos, control de la red y similares. Aún además el sistema se puede usar para detectar o impedir problemas de seguridad con un lenguaje de programación del lado del cliente, tal como
10 JavaScript, VBScript o similares.

Como se apreciará por una persona de experiencia ordinaria en la técnica, el sistema se puede incorporar como una personalización de un sistema existente, un producto adicional, un aparato de procesamiento que ejecuta software,
15 actualizado, un sistema independiente, un sistema distribuido, un método, un sistema de procesamiento de datos un dispositivo para el procesamiento de datos, y/o un producto de programa de computadora. Por consiguiente, cualquier porción del sistema o módulo puede tomar la forma
20 de un aparato de procesamiento que ejecuta el código, una modalidad basada en internet, una modalidad completamente de hardware, o una modalidad que combina aspectos del internet, software y hardware. Adicionalmente, el sistema puede tomar la forma de un producto de programa de computadora en un

medio de almacenamiento legible por computadora que tiene medios de códigos de programa legibles por computadora incorporados en el medio de almacenamiento. Cualquier medio de almacenamiento legible por computadora adecuado se puede
5 utilizar, incluyendo discos duros, CD-ROM, dispositivos de almacenamiento ópticos, dispositivos de almacenamiento magnéticos y/o similares.

El sistema y método se describe en la presente con referencia a capturas de pantalla, diagramas de bloques e
10 ilustraciones de gráfica de flujo de los métodos, aparatos (por ejemplo, sistemas), y productos de programa de computadora de acuerdo con varias modalidades. Se entenderá que cada bloque funcional de los diagramas de bloque y las ilustraciones de la gráfica de flujo, y las combinaciones de
15 los bloques funcionales en los diagramas de bloque y las ilustraciones de la gráfica de flujo, respectivamente, se pueden implementar por instrucciones de programas de computadora.

Estas instrucciones de programa de computadora se pueden
20 cargar en una computadora de propósito general, computadora de propósito especial, u otro aparato de procesamiento de datos programable para producir una máquina, tal que las instrucciones que se ejecutan en la computadora u otro aparato de procesamiento de datos programable crea medios

para implementar las funciones especificadas en el bloque o bloques de la gráfica de flujo. Estas instrucciones de programa de computadora también se pueden almacenar en una memoria legible por computadora que puede elegir una computadora u otro aparato de procesamiento de datos programable al funcionar en una manera particular, tal que las instrucciones almacenadas en la memoria legible por computadora producen un artículo de fabricación incluyendo medios de instrucción que implementan la función especificada en el bloque o bloques del diagrama de la gráfica de flujo. Las instrucciones de programa de computadora también se pueden cargar en una computadora u otro aparato de procesamiento de datos programable para provocar una serie de pasos operacionales que se llevan a cabo en la computadora u otro aparato programable para producir un proceso de implementado por computadora tal que las instrucciones que se ejecutan en la computadora u otro aparato programable proporcionan pasos para implementar las funciones especificadas en el bloque o bloques de la gráfica de flujo.

Por consiguiente, los bloques funciones de los diagramas de bloque y las ilustraciones de la gráfica de flujo soportan combinaciones de medios para llevar a cabo las funciones especificadas, combinaciones de pasos para llevar a cabo las funciones especificadas, y medios de instrucciones de

programa para llevar a cabo las funciones especificadas. También se entenderá que cada bloque funcional de los diagramas de bloque y las ilustraciones de la gráfica de flujo, y las combinaciones de los bloques funcionales en los

5 diagramas de bloques y las ilustraciones de la gráfica de flujo, se pueden implementar ya sea los sistemas de computadora basados en hardware de propósito especial que llevan a cabo las funciones o pasos especificados, o combinaciones adecuadas de instrucciones de hardware y

10 computadora de propósito especial. Además, las ilustraciones de los flujos de proceso y las descripciones de los mismos pueden hacer referencia a las ventajas de usuario, páginas de la red, sitios de la red, formas de la red, instrucciones, etc. Los profesionales apreciarán que los pasos ilustrados

15 descritos en la presente pueden comprender en cualquier número de configuraciones incluyendo el uso de ventanas, páginas de la red, formas de la red, ventanas emergentes, instrucciones y similares. Se debe apreciar adicionalmente que los diversos pasos como se ilustran y se describen se

20 pueden combinar en páginas de la red individuales y/o ventanas pero se han expandido por razones de simplicidad. En otros casos, los pasos ilustrados y descritos como pasos de procesos individuales se pueden separar en varias páginas de la red y/o ventanas pero se han combinado para simplicidad.

El término "no transitorio" se va a entender que remueve solo la propagación de señales transitorias per se del alcance de las reivindicaciones y no cede los derechos a todos los medios legibles por computadora estándares que no son señales transitorias de propagación per se. Establecido de otra manera, el significado del término "medio legible por computadora no transitorio" se debe considerar que excluye solo aquellos tipos de medios legibles por computadora transitorios que se encontraron en *In Re Nuijten* que se encuentran fuera del alcance del contenido patentable bajo 35 U.S.C. § 101.

Los beneficios, otras ventajas y soluciones a los problemas se han descrito en la presente con respecto a las modalidades específicas. Sin embargo, los beneficios, ventajas, soluciones a los problemas, y cualquiera de los elementos que pueden provocar cualquier beneficio, ventaja, o solución que se presenta o que sea más pronunciado no se van a considerar como características críticas, requeridas, esenciales o elementos de la descripción.

Aunque la descripción incluye un método, se contempla que se puede incorporar como instrucciones de programa de computadora en un portador legible por computadora tangible, tal como un disco magnético o de memoria óptica, o magnético u óptico. Todos los equivalentes estructurales, químicos y

funcionales a los elementos de las modalidades ejemplares descritas en lo anterior que son conocidos por aquellas personas de experiencia ordinaria en la técnica se incorporan expresamente en la presente a manera de referencia y se

5 proponen para ser abarcados por las presentes reivindicaciones. Por otra parte, no es necesario para un dispositivo o método abordar cada uno y cada problema buscado para ser resuelto por la presente descripción, para que sea abarcado por las presentes reivindicaciones. Adicionalmente,

10 ningún elemento, componente, o paso de método en la presente descripción se propone para ser dedicado al público sin considerar si el elemento, componente, o paso de método se cita explícitamente en las reivindicaciones. Ningún elemento de reclamación en la presente se va a considerar bajo las

15 provisiones de 35 U.S.C. 112, sexto párrafo, a menos que el elemento se cite expresamente usando la frases "significa para". Como se usa en la presente, los términos "comprende", "que comprende", o cualquier otra variación de los mismos, se proponen para cubrir una inclusión no exclusiva, tal que un

20 proceso, método, artículo, o aparato que comprende la lista de elementos no incluya solo esos elementos sino puede incluir otros elementos que no se listan expresamente o son inherentes a este proceso, método, artículo o aparato.

Donde una frase similar a "al menos uno de A, B, o C",

“al menos uno de A, B, y C”, “uno o más A, B, o C,” o “uno o más de A, B, y C” se usa, se propone se propone que la frase sea interpretada para proponer que A sola puede estar presente en una modalidad, B sola puede estar presente en una
5 modalidad, C sola puede estar presente en una modalidad, o que cualquier combinación de los elementos A, B y C puedan estar presentes en una sola modalidad; por ejemplo, A y B, A y C, B y C, o A y B y C.

Los cambios y modificaciones se pueden hacer a las
10 modalidades descritas sin apartarse del alcance de la presente descripción. Estas otros cambios y modificaciones se proponen para ser incluidos dentro del alcance de la presente descripción, como se expresa en las siguientes reivindicaciones.

15

20