

**REPÚBLICA DE COLOMBIA
SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO**

Oficio N° 12997

Ref. Expediente N° NC2017/0003261

Señor(a)
CATBIRD NETWORKS INC.
notificaciones@clarkemodet.com.co

Asunto: PATENTE DE INVENCION - PCT

Patente de Invención	PT	Patente de Modelo de Utilidad	
Vía Nacional			
Vía PCT (Fase Nacional)	PCT	Capítulo I	Capítulo II
No. Solicitud Internacional	PCT/US2015/044865		
Fecha de Presentación Internacional	12 de agosto de 2015		

Como resultado del examen de fondo realizado, con fundamento en el Artículo 45 de la Decisión 486 de la Comisión de la Comunidad Andina, se comunica:

1. Documentos estudiados

Descripción	NC2017/0003261	3 de abril de 2017
Reivindicaciones:	NC2017/0003261	3 de abril de 2017
	NC2017/0003261	12 de junio de 2017
	NC2017/0003261	6 de agosto de 2018
Dibujos:	NC2017/0003261	3 de abril de 2017
Oposición(es):	No se presentaron	No se presentaron
Respuesta del solicitante:	NC2017/0003261	6 de agosto de 2018
Prioridad(es):	País: US, ESTADOS UNIDOS DE AMÉRICA Número: 62/046,807 Fecha: 5 de septiembre de 2014 País: US, ESTADOS UNIDOS DE AMÉRICA Número: 62/060,433 Fecha: 6 de octubre de 2014 País: US, ESTADOS UNIDOS DE AMÉRICA Número: 14/523,624 Fecha: 24 de octubre de 2014	

2. Análisis de la Prioridad

Se acepta la reivindicación de prioridad porque esta solicitud fue presentada dentro del plazo establecido y el contenido técnico de esta solicitud corresponde con el de la prioridad reivindicada.

**REPÚBLICA DE COLOMBIA
SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO**

Oficio N° 12997

Ref. Expediente N° NC2017/0003261

3. Modificaciones presentadas (Art. 34 D 486 y Art. 19, 22 y 34 PCT)

Se aceptan las modificaciones presentadas comoquiera que se ajustan a las prescripciones contenidas en el reglamento del PCT y en el Art 34 de la Decisión 486

4. Objeto de la invención

De acuerdo con lo establecido en el numeral 1.2.2.2 del Capítulo Primero del Título X de la Circular Única para efectos del examen de patentabilidad, se tendrá en cuenta la tasa pagada por el solicitante al momento de comenzar el examen para las reivindicaciones adicionales; esto es que cuando la solicitud contenga más de diez (10) reivindicaciones y no se haya pagado la tasa complementaria, sólo se estudiarán las cubiertas por la tasa pagada. Por lo tanto, se estudiarán las reivindicaciones 1 a 17 del capítulo reivindicatorio (Radicado NC2017/0003261 del 6 de agosto de 2018).

Título de la solicitud: "SISTEMAS Y MÉTODOS PARA ANÁLISIS Y REPORTE DE RED" (Radicado NC2017/0003261 del 3 de abril de 2017).

El problema planteado en esta solicitud consiste en 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.

Para resolver este problema técnico, la solicitud en estudio proporciona: sistemas y métodos para análisis y reporte de red.

El objeto de la presente solicitud se relaciona con la Clasificación Internacional de Patentes (CIP): H04L 12/26, H04L 12/24.

5. De la solicitud de patente

Reivindicaciones (Art. 30 D 486, Art. 22 PCT)

La expresión: "*pluralidad*", de las reivindicaciones 1 y 16; "*en el que una de las características de una conexión entre recursos de red o una característica de un recurso de red se identifica con base en un atributo seleccionado de los datos recolectados*", de la reivindicación 1; "*uno o más*", de la reivindicación 13; precediendo

REPÚBLICA DE COLOMBIA
SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO

Oficio N° 12997

Ref. Expediente N° NC2017/0003261

una característica no es limitativo, porque hace opcional a la característica y no limita el alcance de la reivindicación.

Las frases: “*de diferentes tipos de fuentes*”, “*atributo seleccionado de los datos recolectados*”, “*una primera zona lógica*”, “*segunda zona lógica*”, de la reivindicación 1; son de carácter general que sugieren de forma imprecisa que la protección se extiende a posibles variaciones o modificaciones.

Los pasajes: “*por el sistema de computadora (800), una gráfica de información de flujo (925) que representa la pluralidad de recursos de la red y las conexiones entre la pluralidad de recursos de la red, en donde la pluralidad de recursos de red incluye el primer recurso de red y la información de flujo del gráfico representa el tráfico de red permitido entre los recursos de la red y el tráfico de la red que está bloqueado entre los recursos de la red; presentar la gráfica de información de flujo (930) a través de una pantalla de una interfaz de usuario en comunicación con el sistema de computadora, en el que el gráfico de información de flujo representa conexiones entre los recursos de red usando líneas de flujo direccional seleccionables; y en respuesta a la selección (935), por un usuario a través de la interfaz de usuario, de una línea de flujo respectiva asociada a una conexión desde la pluralidad de conexiones, mostrando las características de la conexión seleccionada (940) incluyendo reglas de visualización para permitir y bloquear el tráfico sobre la conexión seleccionada.*”, de la reivindicación 1; “*el atributo se selecciona por un usuario a través de la interfaz de usuario*”, de la reivindicación 4; “*la característica de un recurso de la red se indica visualmente en la gráfica de información de flujo*”, de la reivindicación 6; “*indicar visualmente el recurso identificado que se asocia con la vulnerabilidad de seguridad en la gráfica de información de flujo*”, de la reivindicación 10; “*la gráfica de información de flujo representa la información en un recurso y uno o más de: los datos de la red asociados con el recurso, y un atributo operacional del sistema asociado con el recurso*”, de la reivindicación 11; “*actualizar la gráfica de información de flujo (960) basada en los datos actualizados; y presentar la gráfica de información de flujo actualizada (930) a través de la pantalla*”, de la reivindicación 12; “*en el que los datos relacionados con la gráfica de información de flujo incluyen uno o más de: los datos recolectados para generar la gráfica de información de flujo, y la gráfica de información de flujo misma*”, de la reivindicación 13; “*analizar los datos recolectados (970); y generar una alerta (975) en respuesta al análisis de los datos recolectados*”, de la reivindicación 14; “*Un medio legible por computadora no transitorio, tangible (814), caracterizado porque almacena instrucciones que, cuando se ejecutan, provocan que un sistema de computadora (800), genere una gráfica de información de flujo (925)*”

Página 3 de 36

**REPÚBLICA DE COLOMBIA
SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO**

Oficio N° 12997

Ref. Expediente N° NC2017/0003261

que representa la pluralidad de recursos de la red y las conexiones entre la pluralidad de recursos de la red, en donde la pluralidad de recursos de red incluye el primer recurso de red y la información de flujo del gráfico representa el tráfico de red permitido entre los recursos de la red y el tráfico de la red que está bloqueado entre los recursos de la red; presente la gráfica de información de flujo (930) a través de la pantalla de una interfaz de usuario en comunicación con el sistema de computadora, en el que el gráfico de información de flujo representa conexiones entre los recursos de red usando líneas de flujo direccional seleccionables; y en respuesta a la selección (935), por un usuario a través de la interfaz de usuario, de una línea de flujo respectiva asociada a una conexión desde la pluralidad de conexiones, mostrar las características de la conexión seleccionada (940) incluyendo reglas de visualización para permitir y bloquear el tráfico sobre la conexión seleccionada”, de la reivindicación 16 y “genere una gráfica de información de flujo (925) que representa la pluralidad de recursos de la red y las conexiones entre la pluralidad de recursos de la red, en donde la pluralidad de recursos de red incluye el primer recurso de red y la información de flujo del gráfico representa el tráfico de red permitido entre los recursos de la red y el tráfico de la red que está bloqueado entre los recursos de la red; y presente la gráfica de información de flujo (930) a través de una pantalla de una interfaz de usuario en comunicación con el sistema de computadora, en el que el gráfico de información de flujo representa conexiones entre los recursos de red usando líneas de flujo direccional seleccionables; y en respuesta a la selección (935), por un usuario a través de la interfaz de usuario, de una línea de flujo respectiva asociada a una conexión desde la pluralidad de conexiones, mostrar las características de la conexión seleccionada (940) incluyendo reglas de visualización para permitir y bloquear el tráfico sobre la conexión seleccionada”, de la reivindicación 17; sugieren formas de presentar información.

Los fragmentos: “usando líneas de flujo direccional seleccionables”, de la reivindicación 1; “usados para identificar la conexión”, de la reivindicación 7; “usando líneas de flujo direccional seleccionables”, de las reivindicaciones 16 y 17; sugieren un uso.

La reivindicación 8 dice: “método de conformidad con la reivindicación 8”, lo cual es confuso ya que no es claro la dependencia de dicha reivindicación.

**REPÚBLICA DE COLOMBIA
SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO**

Oficio N° 12997

Ref. Expediente N° NC2017/0003261

6. Determinación del Estado de la Técnica

El estado de la técnica se determinó con base en la fecha de presentación de la solicitud de prioridad: 05 de septiembre de 2014, y se encontraron los siguientes documentos que anticipan el objeto de esta solicitud:

Ítem	Documento	Título	Fecha de publicación
D3	US2009327903A1	"System and Method for Network Topology and Flow Visualization"	31 de diciembre de 2009
D4	US7849497B1	"Method and system for analyzing the security of a network"	07 de diciembre de 2010
D5	US2008005784A1	"Proactive network security systems to protect against hackers"	03 de enero de 2008
D6	US2005193430A1	"System and method for risk detection and analysis in a computer network"	01 de septiembre de 2005

El documento D3¹ divulga una vista de topología de una red en una pantalla visual de un sistema informático. La vista de topología incluye objetos de subred, objetos de dispositivo de red y objetos de interfaz dentro de los objetos de dispositivo de red. Los registros de flujo de red se adquieren de cada dispositivo dentro de la red. Los registros de flujo de red separados adquiridos de diferentes dispositivos en la red se correlacionan juntos en un registro de flujo de red común (Resumen).

El documento D4² divulga un método y un sistema para analizar la seguridad de una red de computadoras. De acuerdo con varias implementaciones, hay un adaptador de dispositivo asociado con cada dispositivo que tiene un impacto significativo en la seguridad de la red (por ejemplo, enrutadores, conmutadores, puertas de enlace o "hosts significativos"). El adaptador del dispositivo, que puede implementarse como una pieza de software que se ejecuta de forma remota desde el dispositivo, consulta al dispositivo para determinar cuáles son sus configuraciones de seguridad (por ejemplo, sus reglas de firewall) (Resumen).

El documento D5³ divulga un sistema de seguridad de red proactivo que protege contra piratas informáticos para la defensa automatizada proactiva contra piratas informáticos mediante la búsqueda, el reporte, la comunicación con contramedidas y

1 <https://patents.google.com/patent/US20090327903A1>

2 <https://patents.google.com/patent/US7849497B1>

3 <https://patents.google.com/patent/US20080005784A1>

REPÚBLICA DE COLOMBIA
SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO

Oficio N° 12997

Ref. Expediente N° NC2017/0003261

la eliminación de las vulnerabilidades y exposiciones comunes (CVE) que explotan (Resumen).

El documento D6⁴ divulga sistemas y métodos de detección y análisis de riesgos en una red informática. Se pueden proporcionar sistemas y métodos computarizados y automatizados. La información de vulnerabilidad sin formato y la información de red se pueden utilizar para determinar la información de vulnerabilidad real asociada con los nodos de la red. Se proporcionan métodos en los cuales se modelan las redes de computadoras y los modelos utilizados para realizar simulaciones de ataques y determinar los riesgos asociados con las vulnerabilidades. Los riesgos se pueden evaluar y priorizar, y se puede proporcionar información sobre los arreglos (Resumen).

7. Examen de Patentabilidad (Art. 14 D486)

Novedad (Art 16 D486)

La reivindicación 1 consiste en: “*Un método para calcular el análisis de red, caracterizado porque comprende las etapas de (...)*” (Radicado NC2017/0003261 del 6 de agosto de 2018).

Comparación de las características esenciales con el estado de la técnica.

Características esenciales	D3	D4
Un método para calcular el análisis de red, caracterizado porque comprende las etapas de (...)	Se genera una vista de topología de una red en una pantalla visual de un sistema informático. La vista de topología incluye objetos de subred, objetos de dispositivo de red y objetos de interfaz dentro de los objetos de dispositivo de red. Los registros de flujo de red se adquieren de cada dispositivo dentro de la red. Los registros de flujo de red separados adquiridos de diferentes dispositivos en la red se correlacionan juntos en un registro de flujo de red común (Resumen).	Aquí se describe un método y un sistema para analizar la seguridad de una red de computadoras. De acuerdo con varias implementaciones, hay un adaptador de dispositivo asociado con cada dispositivo que tiene un impacto significativo en la seguridad de la red (por ejemplo, enrutadores, conmutadores, puertas de enlace o "hosts significativos"). El adaptador del dispositivo, que puede implementarse como una pieza de software que se ejecuta de forma remota desde el dispositivo, consulta al dispositivo para determinar cuáles son sus configuraciones de seguridad

⁴ <https://patents.google.com/patent/US20050193430A1>

REPÚBLICA DE COLOMBIA
SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO

Oficio N° 12997

Ref. Expediente N° NC2017/0003261

		(por ejemplo, sus reglas de firewall) (Resumen).
Recolectar (905), por un sistema de computadora (800), datos de una pluralidad de diferentes tipos de fuentes, en donde los datos recolectados incluyen datos de la red y datos de recurso.	La correlación de los flujos de red de dispositivo a dispositivo requiere algún almacenamiento de datos de flujo de red, ya que la llegada de datos de flujo de red al módulo de correlación (1119) de diferentes dispositivos puede variar en el tiempo, dependiendo de las técnicas utilizadas para recopilar el flujo de red datos. Además, es posible que se requiera el almacenamiento en caché de los datos de flujo de la red para evitar la pérdida prematura de los datos de flujo de la red antes de que se puedan representar visualmente en la GUI (1300) (Párrafo 0090).	En algún momento, antes o después de que el usuario inicie el programa de análisis de seguridad (14), los adaptadores de dispositivo (90), (92) y (94) recuperan la información de configuración de sus dispositivos respectivos (91), (93) y (95). Los ejemplos de información de configuración recopilada incluyen reglas de control de acceso, reglas de autenticación y reglas para verificar la integridad de los datos. El adaptador de dispositivo puede obtener este tipo de datos en forma de reglas de firewall almacenadas en el dispositivo con el que está asociado (Columna 5, Líneas 23 a 30).
Identificar, por el sistema de computadora (800) 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 (915) relacionados con el evento de tráfico de la red.	El método también incluye una operación (1803) para analizar los datos de configuración del dispositivo adquiridos para identificar una o más interfaces de cada número de dispositivos de red, y para identificar subredes a las que se conectan una o más interfaces (Párrafo 0102).	Hay muchas formas posibles de generar la información de topología contenida en la base de datos de topologías (58). En una realización, la topología se crea a través de un proceso manual, en el que el usuario identifica todos los segmentos de red y dispositivos que se utilizarán en la topología. El usuario también crea una definición de red o host para cada elemento de la topología. El usuario coloca cada red o dispositivo en el diagrama de topología (Columna 4, Líneas 14 a 21).
Identificar, por el sistema de computadora (800) con base en los datos de recurso en los datos recolectados, conexiones entre la pluralidad de recursos de la red (920); en el que una de las características de una conexión entre recursos de red o una característica de un recurso de red se identifica con base en un atributo seleccionado de los datos recolectados.	Los segmentos de línea representan conexiones de red a través de las cuales se transmitirán los flujos de red. Además, en una realización, se realiza una operación para representar en la visualización visual una vista jerárquica del número de dispositivos de red y las interfaces dentro del número de dispositivos de red. También en esta realización, tras la selección de un dispositivo de red particular en la vista jerárquica, se representa una vista aislada del dispositivo de red seleccionado particular en la pantalla visual (Párrafo 0104).	El programa de análisis de seguridad (14) luego determina la naturaleza de las conexiones entre redes y dispositivos basándose en parte en los rangos de direcciones de red de las redes y las direcciones de Protocolo de Internet (IP) de las interfaces de red asociadas con los dispositivos. En otra realización, el programa de análisis de seguridad (14) descubre automáticamente la topología utilizando una herramienta de descubrimiento de topología convencional y varias herramientas de gestión de red (Columna 4, Líneas 22 a 30).

REPÚBLICA DE COLOMBIA
SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO

Oficio N° 12997

Ref. Expediente N° NC2017/0003261

En respuesta a la detección, basada en los datos recolectados (905), un cambio en un atributo (420) de, un primer recurso de red asociado con una primera zona lógica, moviendo (430) el primer recurso de red de la primera zona lógica a una segunda zona lógica.	La GUI (1300) incluye una primera región de visualización (1303) dentro de la cual se representa visualmente la visualización de la topología de la red (1113). Los dispositivos de red (1104A) - (1104C) se muestran como círculos grandes (Párrafo 0076).	La red de computadoras, generalmente etiquetada (10) incluye una computadora (12) en la que se ejecuta el programa de análisis de seguridad (14). La red de computadoras (10) también incluye las puertas de enlace primera y segunda (16) y (18), y tres "hosts significativos" (20), (22) y (24). Tal como se usa en el presente documento, el término "host significativo" significa cualquier host que almacene valiosos activos de información o ejecute software que sea crítico para el funcionamiento del negocio de la entidad que utiliza la red (10) (incluidos comerciales, públicos / gubernamentales o no - entidades lucrativas) (Columna 3, líneas 12 a 20).
El movimiento comprende actualizar una base de datos para indicar que, el primer recurso de red es un miembro de la segunda zona lógica, y en base a la membresía en la segunda zona lógica, la comunicación entre el primer recurso de red y otros recursos de red está bloqueada.	La información de flujo de red que el sistema 1100 recopila con el tiempo puede almacenarse en una base de datos. Esta información histórica del flujo de la red se puede analizar a través de varios métodos y técnicas de extracción de datos. En una realización, se pueden generar visualizaciones históricas dentro de la GUI 1300 para mostrar tendencias de una manera espacial dentro de la vista de topología de red (Párrafo 0095).	Hay muchas formas posibles de generar la información de topología contenida en la base de datos de topologías (58). En una realización, la topología se crea a través de un proceso manual, en el que el usuario identifica todos los segmentos de red y dispositivos que se utilizarán en la topología. El usuario también crea una definición de red o host para cada elemento de la topología (Columna 4, Líneas 14 a 20).
Generar, por el sistema de computadora (800), una gráfica de información de flujo (925) que representa la pluralidad de recursos de la red y las conexiones entre la pluralidad de recursos de la red, en donde la pluralidad de recursos de red incluye el primer recurso de red y la información de flujo del gráfico representa el tráfico de red permitido entre los recursos de la red y el tráfico de la red que está bloqueado entre los recursos de la red.	El módulo de visualización de red se define además para representar en una pantalla visual una vista de topología de la red que incluye representaciones gráficas de los dispositivos, interfaces dentro de los dispositivos y conexiones entre las interfaces y las subredes. El sistema también incluye un módulo de gestión de recolección de flujo de red definido para adquirir registros de flujo de red de cada dispositivo dentro de la red (Párrafo 0006).	Un método para analizar la seguridad de una red informática, que comprende: recopilar los ajustes de configuración de seguridad de cada uno de una pluralidad de nodos de la red informática, para cada nodo: abrir una sesión de comunicación con el nodo, consultar el nodo utilizando la sesión de comunicación para determinar las configuraciones de configuración de seguridad del nodo; y obtener reglas que cada uno de los nodos utiliza para admitir o denegar el tráfico de red; mostrar gráficamente la topología de la red en una interfaz de usuario al mostrar una representación para cada uno de los nodos en la red y mostrar las conexiones entre las

REPÚBLICA DE COLOMBIA
SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO

Oficio N° 12997

Ref. Expediente N° NC2017/0003261

		representaciones, las conexiones son representativas de las rutas de comunicación entre cada uno de los nodos (Reivindicación 1).
Presentar la gráfica de información de flujo (930) a través de una pantalla de una interfaz de usuario en comunicación con el sistema de computadora, en el que el gráfico de información de flujo representa conexiones entre los recursos de red usando líneas de flujo direccional seleccionables.	El módulo de visualización de red (1109) se define además para representar en una pantalla visual de un sistema informático, una visualización de topología de red (1113) que incluye una vista de topología de la red (1102), que incluye representaciones gráficas de los dispositivos (1104), las interfaces (1101) dentro de los dispositivos (1101), y varias conexiones entre las interfaces (1101) y las subredes. Las interfaces lógicas, como el bucle de retorno del enrutador, la interfaz nula, la interfaz local, la interfaz VLAN, los túneles, etc., también se muestran en la visualización de la topología de la red (1113) (Párrafo 0075).	El método de la reivindicación 1, en el que el paso de visualización gráfica comprende visualizar un icono como la representación de cada uno de los nodos en la red y visualizar líneas como las conexiones entre los iconos, siendo las líneas representativas de las rutas de comunicación entre los nodos (Reivindicación 4).
Y en respuesta a la selección (935), por un usuario a través de la interfaz de usuario, de una línea de flujo respectiva asociada a una conexión desde la pluralidad de conexiones, mostrando las características de la conexión seleccionada (940) incluyendo reglas de visualización para permitir y bloquear el tráfico sobre la conexión seleccionada.	Un usuario puede seleccionar el dispositivo particular (1609) dentro de la vista jerárquica de la red dentro de la segunda región de pantalla (1305). Una vista aislada del dispositivo seleccionado (1609) se representa en la primera región de pantalla (1303) que muestra el dispositivo (1609) junto con sus interfaces y flechas que representan los diversos flujos de red asociados con el dispositivo (1609) (Párrafo 0092).	En el que el dispositivo de interfaz de usuario comprende un módulo de interfaz de usuario que realiza pasos que comprenden: recibir una selección de usuario del primer dispositivo y del segundo dispositivo; mostrar, para el usuario, la política de ruta de seguridad derivada en forma de árbol, el árbol está estructurado según el orden de clasificación de los criterios; recibir, del usuario, una solicitud para cambiar el orden de clasificación de los criterios; y volver a mostrar el árbol al usuario en función del orden de clasificación modificado (Reivindicación 12).

Adicionalmente los documentos D5 y D6 divulgan las características esenciales de la invención a continuación:

Comparación de las características esenciales con el estado de la técnica

Características esenciales	D5	D6
Un método para calcular el análisis de red,	Un sistema de seguridad de red proactivo que protege contra piratas	La presente invención proporciona sistemas y métodos para la detección

**REPÚBLICA DE COLOMBIA
SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO**

Oficio N° 12997

Ref. Expediente N° NC2017/0003261

caracterizado porque comprende las etapas de (...)	informáticos para la defensa automatizada proactiva contra piratas informáticos mediante la búsqueda, el reporte, la comunicación con contramedidas y la eliminación de las vulnerabilidades y exposiciones comunes (CVE) que explotan (Resumen).	y análisis de riesgos en una red informática. Se pueden proporcionar sistemas y métodos computarizados y automatizados. La información de vulnerabilidad sin formato y la información de red se pueden utilizar para determinar la información de vulnerabilidad real asociada con los nodos de la red. Se proporcionan métodos en los cuales se modelan las redes de computadoras y los modelos utilizados para realizar simulaciones de ataques y determinar los riesgos asociados con las vulnerabilidades. Los riesgos se pueden evaluar y priorizar, y se puede proporcionar información sobre los arreglos (Resumen).
Recolectar (905), por un sistema de computadora (800), datos de una pluralidad de diferentes tipos de fuentes, en donde los datos recolectados incluyen datos de la red y datos de recurso.	En funcionamiento, el hardware está conectado a una red basada en computadora a través de los medios estándar de conectividad que incluyen, entre otros, una conexión TCP / IP por cable o inalámbrica. A continuación, el administrador lo configura rápidamente a través de la GUI segura. Una vez configurado, el sistema puede explorar opcionalmente la red de acceso local para determinar la topología de la red y recopilar información sobre el sistema operativo y la dirección IP (Párrafo 0050).	De acuerdo con algunos aspectos de la presente invención, se proporcionan métodos para realizar una evaluación de vulnerabilidad automatizada en una red de computadoras, los métodos que involucran la recopilación de información sobre la red y sus componentes, creando un modelo de la red (que puede incluir todos sus nodos y sus configuraciones / servicios), simulando posibles ataques contra la red utilizando gráficos de ataques, generando las consecuencias correspondientes de posibles ataques, calculando la probabilidad de que ocurran ataques y clasificando las vulnerabilidades asociadas con posibles ataques (Párrafo 0012).
Identificar, por el sistema de computadora (800) 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 (915) relacionados con el evento de tráfico de la red.	El método de la reivindicación 12, en el que la lista de activos identifica puertos abiertos para cada uno de los uno o más activos (Reivindicación 5).	El algoritmo puede primero identificar o seleccionar nodos de puntos de inicio para los ataques. El algoritmo puede utilizar la información de restricción asociada con los nodos del gráfico de conexión para determinar posibles rutas de ataque desde los nodos del gráfico de punto de inicio a través de otros nodos del gráfico de conexión, y para determinar los nodos del gráfico de punto de terminación del ataque (Párrafo 0013).

REPÚBLICA DE COLOMBIA
SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO

Oficio N° 12997

Ref. Expediente N° NC2017/0003261

Identificar, por el sistema de computadora (800) con base en los datos de recurso en los datos recolectados, conexiones entre la pluralidad de recursos de la red (920); en el que una de las características de una conexión entre recursos de red o una característica de un recurso de red se identifica con base en un atributo seleccionado de los datos recolectados.	El método de la reivindicación 12, en el que para cada uno de los uno o más activos, la lista identifica una o más de una dirección de control de acceso a medios, información de aplicación, información de sesión, información de transporte, información de socket y un tipo de conexión (Reivindicación 6).	Los agentes de descubrimiento (158) recopilan información de red con respecto a vulnerabilidades sin formato, topología, servicios y otra información. Los agentes de descubrimiento ejemplares (158) incluyen agentes de firewall, agentes de topología de red, agentes de servicio, agentes de escáner de vulnerabilidad en bruto y otros agentes. Los agentes especializados recopilan información específica de nodos de red específicos. Por ejemplo, los agentes de firewall, por ejemplo, recopilan listas de control de acceso y conjuntos de reglas de filtrado; Los agentes de topología de red recopilan información sobre las interconexiones entre los dispositivos de red y los hosts (Párrafo 0060).
En respuesta a la detección, basada en los datos recolectados (905), un cambio en un atributo (420) de un primer recurso de red asociado con una primera zona lógica, moviendo (430) el primer recurso de red de la primera zona lógica a una segunda zona lógica.	En el caso de que la contramedida de INFOSEC sea un IPS, una alerta dinámica del administrador de TI o un destinatario de alerta alternativo y se realizarán cambios dinámicos en la lista de acceso a IPS a través del complemento del cliente de comunicaciones de contramedidas que se ha escrito específicamente para ese MAKE, MODELO y VERSION IPS. En el caso de que la contramedida de INFOSEC sea un IDS, una alerta dinámica del administrador de TI o un receptor de alerta alternativo y compartir los datos de pruebas CVE relacionados con el IDS para ayudar al IDS a reducir los falsos positivos en el módulo de alerta del IDS, así como a reducir la carga de tráfico. relacionado con las detecciones de intrusión que atacan una dirección IP particular que no es susceptible a esa metodología de ataque particular basada en los datos de pruebas CVE relacionados y se llevará a cabo a través del complemento de cliente de comunicaciones de contramedidas que se ha escrito específicamente	Se envían paquetes de datos a cada dispositivo de red y se interpretan las respuestas recibidas de los dispositivos de red para determinar si existe una vulnerabilidad sin formato. Por ejemplo, un agente de descubrimiento de información podría realizar pruebas para determinar si una versión particular de BIND vulnerable a los ataques está presente. El agente de descubrimiento de información enviaría paquetes que contengan un comando de consulta para que el servidor BIND en una red devuelva su número de versión (Párrafo 0067). El método de la reivindicación 44, en el que generar un gráfico de ataque usando un algoritmo de línea frontal móvil comprende: seleccionar uno o más primeros nodos de gráfico; determinar, para un segundo nodo gráfico, si las restricciones en el estado de servicio asociado con el segundo nodo gráfico están satisfechas por el estado de uno o más primeros nodos gráficos; y agregar un borde que conecta uno o más primeros nodos de gráfico al

**REPÚBLICA DE COLOMBIA
SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO**

Oficio N° 12997

Ref. Expediente N° NC2017/0003261

	para ese MAKE, MODELO y VERSIÓN IDS (Párrafo 0057).	segundo nodo de gráfico si las restricciones en el estado de servicio asociado con el segundo nodo de gráfico se satisfacen con el estado de uno o más primeros nodos de gráfico (Reivindicación 18).
El movimiento comprende actualizar una base de datos para indicar que el primer recurso de red es un miembro de la segunda zona lógica, y en base a la membresía en la segunda zona lógica, la comunicación entre el primer recurso de red y otros recursos de red está bloqueada.	Estos complementos del motor INFOSEC pueden incluir nuevas interfaces para varias contramedidas (es decir, firewalls, VPNs, IDS e IPS), funcionalidad de auditoría CVE nueva o mejorada, informes de cumplimiento normativo mejorado o nuevo, herramientas de creación de políticas nuevas o mejoradas, capacidades de auditoría mejoradas como la tecnología inalámbrica fraudulenta. Detección de dispositivos, detección de dispositivos móviles, tablas de bases de datos actualizadas, funciones de GUI actualizadas y otras mejoras "empaquetadas" para mantener la modernidad del sistema (Párrafo 0060).	El administrador de recopilación (144) es responsable de coordinar la recopilación de datos de red realizada por los agentes de descubrimiento (158). El administrador de control (144) activa los agentes, extrae la información recibida por los agentes de acuerdo con las reglas almacenadas en la base de datos de reglas (172) y la base de datos de configuración (174), y actualiza la base de datos de red y servicios (160) con los cambios y la información recibida. De los agentes de descubrimiento (158) (Párrafo 0059).
Generar, por el sistema de computadora (800), una gráfica de información de flujo (925) que representa la pluralidad de recursos de la red y las conexiones entre la pluralidad de recursos de la red, en donde la pluralidad de recursos de red incluye el primer recurso de red y la información de flujo del gráfico representa el tráfico de red permitido entre los recursos de la red y el tráfico de la red que está bloqueado entre los recursos de la red.	Volviendo ahora de forma descriptiva a los dibujos, en los que los caracteres de referencia similares denotan elementos similares en las distintas vistas, las figuras adjuntas ilustran un sistema de seguridad de red proactivo para protegerse contra piratas informáticos, que comprende una interfaz gráfica de usuario (GUI) de factores humanos en diseño (HFID) para la configuración y administración seguras (Párrafo 0039).	El método de la reivindicación 29, en el que generar un gráfico de ataque comprende usar un algoritmo de primera línea móvil (Reivindicación 17).
Presentar la gráfica de información de flujo (930) a través de una pantalla de una interfaz de usuario en comunicación con el sistema de computadora, en el que el gráfico de información de flujo	Una vez que haya iniciado sesión en la GUI segura, un administrador puede navegar rápida y fácilmente a través de los botones gráficos y el texto del hipervínculo. La navegación está optimizada para los medios más rápidos de configuración, operación y administración de un sistema de	El método de la reivindicación 44, en el que generar un gráfico de ataque usando un algoritmo de línea frontal móvil comprende: seleccionar uno o más primeros nodos de gráfico; determinar, para un segundo nodo gráfico, si las restricciones en el estado de servicio asociado con el

**REPÚBLICA DE COLOMBIA
SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO**

Oficio N° 12997

Ref. Expediente N° NC2017/0003261

representa conexiones entre los recursos de red usando líneas de flujo direccional seleccionables.	seguridad de red proactivo Anti-Hacker (Párrafo 0040).	segundo nodo gráfico están satisfechas por el estado de uno o más primeros nodos gráficos; y agregar un borde que conecta uno o más primeros nodos de gráfico al segundo nodo de gráfico si las restricciones en el estado de servicio asociado con el segundo nodo de gráfico se satisfacen con el estado de uno o más primeros nodos de gráfico (Reivindicación 18).
Y en respuesta a la selección (935), por un usuario a través de la interfaz de usuario, de una línea de flujo respectiva asociada a una conexión desde la pluralidad de conexiones, mostrando las características de la conexión seleccionada (940) incluyendo reglas de visualización para permitir y bloquear el tráfico sobre la conexión seleccionada.	El panel de control administrativo proporciona acceso y control de operaciones avanzadas de alerta, como alertas a través del correo electrónico o módulo de buscapersonas al finalizar el descubrimiento de activos basado en la red. El panel de control administrativo proporciona acceso y control de operaciones avanzadas de alerta, como alertas a través de correo electrónico o módulo de buscapersonas al finalizar la prueba CVE en uno o más activos seleccionados de la red en una base por dirección IP (Párrafo 0063).	

De acuerdo con las dos tablas anteriores, las características esenciales del método de la reivindicación 1 habían sido divulgadas previamente en los documentos D3 a D6, por lo tanto, la materia reivindicada no es nueva.

Asimismo, los documentos D3 a D6 divulga las características de las reivindicaciones dependientes así:

- Reivindicación 2: Una red determinada puede incluir una gran cantidad de dispositivos de red diversos. Dichos dispositivos de red pueden incluir, entre otros, enrutadores, concentradores de red, conmutadores, repetidores, tarjetas de interfaz de red y otra infraestructura de red relacionada (Párrafo 0003 del documento D3).

La invención se dirige generalmente a un método y sistema para analizar la seguridad de una red informática. De acuerdo con varias realizaciones de la invención, hay un adaptador de dispositivo asociado con cada dispositivo que tiene un impacto significativo en la seguridad de la red (por ejemplo, enrutadores, conmutadores, puertas de enlace o "hosts significativos") (Columna 2, Líneas 43 a 48 del documento D4).

La alta disponibilidad del sistema de seguridad de red proactiva Anti-Hacker se logra a través de patrones de ritmo cardíaco similares a los humanos para compartir bits y sincronizar el reloj de más de un sistema a través de uno de los

**REPÚBLICA DE COLOMBIA
SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO**

Oficio N° 12997

Ref. Expediente N° NC2017/0003261

muchos medios posibles, que incluyen, entre otros, la comunicación basada en IP a través de una red basada en computadora. Cables, concentradores, conmutadores, enrutadores u otros dispositivos o conectividad serie o USB con o sin cables cruzados según sea necesario (Párrafo 0046 del documento D5).

Como se muestra, la red tiene dos conexiones de proveedor de servicios de Internet ("ISP") (230) y (236), dos enrutadores (232) y (238), dos firewalls (234) y (240), una granja de servidores web (246), (248) y (250), una granja de servidores de aplicaciones (262), (264) y (266), dos servidores de base de datos (272) y (274), tres servidores de equilibrio de carga (242), (258) y (268), un servidor FTP (252), un servidor SMTP (256), un servidor de administración (254) y tres dispositivos de red como los conmutadores (244), (260) y (270) (Párrafo 0074 del documento D6).

- Reivindicación 3: El módulo de visualización de red (1109) proporciona el filtrado de los flujos de red mostrados en función de diversos parámetros de flujo de red como DSCP, puerto, dirección IP, protocolo de capa (4), rango de velocidad de bits, rango de bytes, entre otros (Párrafo 0093 del documento D3).

También se puede aplicar un filtro al árbol de políticas para permitir que el usuario se centre en ciertos aspectos de la política de seguridad. El filtro se puede aplicar en función de cualquiera de los cinco criterios de la política. Por ejemplo, si el usuario solo desea saber qué solicitudes HTTP se permiten desde la red interna a la red de usuario, entonces el usuario aplicará un filtro que muestra solo aquellas partes del árbol de políticas que se relacionan con las comunicaciones cuyo puerto de origen es 80 (el puerto HTTP) (Columna 8, Líneas 8 a 16 del documento D4).

En el caso de que la contramedida de INFOSEC sea un cortafuegos o un enrutador de filtrado de tráfico, las alertas dinámicas del administrador de TI o un receptor de alerta alternativo y los cambios dinámicos en la tabla de reglas del cortafuegos se realizarán a través del complemento de cliente de comunicaciones de contramedidas que se ha escrito para eso HAGA, MODELO y VERSIÓN firewall o enrutador de filtrado de tráfico (Párrafo 0055 del documento D5).

El motor analítico (146) recupera la topología de red y la información de servicios de la base de datos de red y servicios (160) y filtra la información para corregir cualquier error, paso (210). Por ejemplo, los agentes de descubrimiento (158) podrían no ser capaces de identificar el número de versión particular o el tipo de sistema operativo y solo indican que Unix es el sistema operativo (Párrafo 0070 del documento D6).

- Reivindicación 4: Un usuario puede seleccionar el dispositivo particular (1609) dentro de la vista jerárquica de la red dentro de la segunda región de pantalla (1305). Una vista aislada del dispositivo seleccionado (1609) se representa en la

**REPÚBLICA DE COLOMBIA
SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO**

Oficio N° 12997

Ref. Expediente N° NC2017/0003261

primera región de pantalla (1303) que muestra el dispositivo (1609) junto con sus interfaces y flechas que representan los diversos flujos de red asociados con el dispositivo (1609). La vista de nivel de dispositivo también proporciona una lista tabular de datos para los flujos de red asociados con el dispositivo (1609) dentro de una región de visualización (1611) (Párrafo 0092 del documento D3).

De acuerdo con esta característica, el usuario puede seleccionar, a través de la interfaz de usuario, un nodo o subred y, al hacer clic en el botón Analizar host, el programa de análisis de seguridad (14) mostrará la seguridad correspondiente al host seleccionado (Columna 8, Líneas 38 a 42 del documento D4).

Una vez que haya iniciado sesión en la GUI segura, un administrador puede navegar rápida y fácilmente a través de los botones gráficos y el texto del hipervínculo. La navegación está optimizada para los medios más rápidos de configuración, operación y administración de un sistema de seguridad de red proactivo Anti-Hacker (Párrafo 0040 del documento D5).

La interfaz de la aplicación (152) también admite una interfaz gráfica de usuario ("GUI") en las computadoras cliente (156) o se proporciona a través del software cliente, lo que permite a los usuarios de las computadoras cliente o software cliente realizar la edición de reglas, configurar informes programados y alertas, para realizar análisis interactivos, edición y navegación del modelo de red, vulnerabilidades y resultados de análisis, para ver el estado de seguridad de la red, para realizar la administración de usuarios, para realizar la administración de tareas, para realizar la administración de agentes y para realizar otras Actividades en comunicación con el software del servidor. En algunas realizaciones, la GUI del cliente está codificada por colores según los riesgos presentados por las vulnerabilidades detectadas (Párrafo 0064 del documento D6).

- Reivindicación 5: Además, en una realización, los flujos de red históricos para un tiempo particular de interés se pueden representar en la vista de topología de red dentro de la GUI (1300) mediante un control deslizante que permite la selección de un período de tiempo particular. Además, se proporciona una función de reproducción automática para permitir la animación de flujos de red históricos a lo largo del tiempo dentro del contexto visual de la vista de topología de red (Párrafo 0096 del documento D3).

Las comunicaciones de contramedidas opcionales se pueden configurar a través de la GUI segura o de forma remota a través de la GUI administrativa del sistema de contramedidas integrado. Se generará un informe de vulnerabilidad automatizado y se notificará al administrador sobre qué CVE existen en qué sistemas e instrucciones simplificadas sobre cómo remediar cada uno de los CVE encontrados (Párrafo 0050 del documento D5).

Página 15 de 36

**REPÚBLICA DE COLOMBIA
SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO**

Oficio N° 12997

Ref. Expediente N° NC2017/0003261

- Reivindicación 6: El módulo de visualización de red se define además para representar en una pantalla visual una vista de topología de la red que incluye representaciones gráficas de los dispositivos, interfaces dentro de los dispositivos y conexiones entre las interfaces y las subredes (Párrafo 0006 del documento D3). Un método para analizar la seguridad de una red informática, que comprende: recopilar los ajustes de configuración de seguridad de cada uno de una pluralidad de nodos de la red informática, para cada nodo: abrir una sesión de comunicación con el nodo, consultar el nodo utilizando la sesión de comunicación para determinar las configuraciones de configuración de seguridad del nodo; y obtener reglas que cada uno de los nodos utiliza para admitir o denegar el tráfico de red; mostrar gráficamente la topología de la red en una interfaz de usuario al mostrar una representación para cada uno de los nodos en la red y mostrar las conexiones entre las representaciones, las conexiones son representativas de las rutas de comunicación entre cada uno de los nodos (Reivindicación 1 del documento D4).
- Reivindicación 7: Cada caso de prueba se define según la configuración del DUT (205) según lo establecido a través de la herramienta de control de red (201) y el tráfico de red proporcionado como entrada al DUT (205) del generador de prueba (203). En la realización donde el DUT (205) es un enrutador, la configuración se puede caracterizar por los siguientes parámetros: número de modelo del enrutador, sistema operativo del enrutador, hardware del enrutador, tipo y tamaño de memoria, política del enrutador, etc. Además, en la realización donde El DUT (205) es un enrutador, el tráfico de la red de entrada se puede caracterizar por los siguientes parámetros: tipo de paquete, longitud del paquete, puerto de origen, puerto de destino, velocidad de datos, características de flujo de datos, etc. (Párrafo 0041 del documento D3).
La unidad de control (142) también sirve como interfaz para y dirige el flujo de datos desde la base de datos de red y servicios (160), la base de datos de vulnerabilidades (162), la base de datos de violaciones (164), la base de datos de ataques (166), la base de datos de riesgos. (168), la base de datos de arreglos (170), la base de datos de reglas (172) y la base de datos de configuración (174) (Párrafo 0058 del documento D5).
- Reivindicación 8: El módulo de visualización de red (1109) se define además para representar en una pantalla visual de un sistema informático, una visualización de topología de red (1113) que incluye una vista de topología de la red (1102), que incluye representaciones gráficas de los dispositivos (1104), las interfaces (1101) dentro de los dispositivos (1101), y varias conexiones entre las interfaces (1101) y las subredes. Las interfaces lógicas, como el bucle de retorno del enrutador, la

**REPÚBLICA DE COLOMBIA
SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO**

Oficio N° 12997

Ref. Expediente N° NC2017/0003261

interfaz nula, la interfaz local, la interfaz VLAN, los túneles, etc., también se muestran en la visualización de la topología de la red (1113) (Párrafo 0075 del documento D3).

El programa de análisis de seguridad (14) luego determina la naturaleza de las conexiones entre redes y dispositivos basándose en parte en los rangos de direcciones de red de las redes y las direcciones de Protocolo de Internet (IP) de las interfaces de red asociadas con los dispositivos. En otra realización, el programa de análisis de seguridad 14 descubre automáticamente la topología usando una herramienta de descubrimiento de topología convencional y varias herramientas de gestión de red (Columna 4, Líneas 22 a 30 del documento D4).

La lista puede contener otra información, como la dirección de control de acceso a medios (MAC) de dichos activos basados en la red, ya sea que la conexión sea por cable o inalámbrica de dichos activos basados en la red y otra información sobre la estructura de la red y sus dispositivos componentes (Párrafo 0034 del documento D5).

La información se recopila de los hosts y la infraestructura de la red, incluidos firewalls, enrutadores, otros escáneres, sistemas de detección de intrusos y software de administración de redes. Además, estos agentes utilizan el ping, el escaneo de puertos, traceroute, arp-walk y otras técnicas conocidas para mapear la topología de la red, incluidas las interconexiones entre los dispositivos de red y los hosts, los tipos de dispositivos de red y hosts, y los servicios que se ejecutan en cada dispositivo de red. y el anfitrión. Esta información se almacena en la base de datos de red y servicios (160), paso (205) (Párrafo 0069 del documento D6).

- Reivindicación 9: Más específicamente, cada hoja en el árbol representa una ruta por la cual se permite al menos algo de tráfico de red. Por el contrario, para cada uno de estos caminos, hay una hoja correspondiente. El usuario puede seleccionar una de las hojas del árbol (110) y hacer clic en la pestaña "Detalles" (Columna 6, Líneas 35 a 39 del documento D4).

Esto puede deshabilitar, desactivar o bloquear temporalmente el acceso a la red, ya sea granular mente a través de los datos CVE relacionados con el Puerto o no granular mente, bloqueando todo el tráfico de dicho activo basado en la red que contiene los CVE (s) que necesitan remediación (Párrafo 0056 del documento D5).

Un método para determinar los puntos de inicio para realizar una evaluación de riesgos en una red informática, que comprende: recopilar un conjunto de listas de control de acceso y reglas de filtrado de uno o más dispositivos de red en la red informática; y analizar el conjunto de listas de control de acceso y las reglas de filtrado para determinar el posible tráfico entrante que representa los posibles

**REPÚBLICA DE COLOMBIA
SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO**

Oficio N° 12997

Ref. Expediente N° NC2017/0003261

puntos de inicio para posibles ataques a la red (Reivindicación 21 del documento D6).

- Reivindicación 10: La tabla de información de dispositivo de ejemplo (1107) incluye una identificación de cada interfaz (1101) dentro de cada dispositivo (1104). Para cada interfaz identificada (1101), la tabla de información del dispositivo de ejemplo (1107) también incluye un nombre, un tipo, una dirección y una máscara de subred. Sin embargo, debe entenderse que la información particular incluida en la tabla de información del dispositivo (1107) puede variar en diferentes formas de realización, siempre que los diversos dispositivos de red (1104) y sus interfaces (1101) a través de los cuales viajan los flujos de red puedan ser únicos. Identificado (Párrafo 0074 del documento D3).

Hay muchas formas posibles de generar la información de topología contenida en la base de datos de topologías (58). En una realización, la topología se crea a través de un proceso manual, en el que el usuario identifica todos los segmentos de red y dispositivos que se utilizarán en la topología. El usuario también crea una definición de red o host para cada elemento de la topología (Columna 4, Líneas 14 a 20 del documento D4).

Un sistema para la seguridad de la red, que comprende: un motor de mapeo dinámico que monitorea los activos en una red y detecta cuando un activo se agrega o se elimina de la red, el motor de mapeo dinámico proporciona datos de identificación de activos (Reivindicación 18 del documento D5).

- Reivindicación 11: El módulo de visualización de red (1109) se define además para representar en una pantalla visual de un sistema informático, una visualización de topología de red (1113) que incluye una vista de topología de la red (1102), que incluye representaciones gráficas de los dispositivos (1104), las interfaces (1101) dentro de los dispositivos (1101), y varias conexiones entre las interfaces (1101) y las subredes. Las interfaces lógicas, como el bucle de retorno del enrutador, la interfaz nula, la interfaz local, la interfaz VLAN, los túneles, etc., también se muestran en la visualización de la topología de la red (1113) (Párrafo 0075 del documento D3).

El método de la reivindicación 1, en el que el paso de visualización gráfica comprende visualizar un icono como la representación de cada uno de los nodos en la red y visualizar líneas como las conexiones entre los iconos, siendo las líneas representativas de las rutas de comunicación entre los nodos (Reivindicación 4 del documento D4).

Una vez que haya iniciado sesión en la GUI segura, un administrador puede navegar rápida y fácilmente a través de los botones gráficos y el texto del

**REPÚBLICA DE COLOMBIA
SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO**

Oficio N° 12997

Ref. Expediente N° NC2017/0003261

hipervínculo. La navegación está optimizada para los medios más rápidos de configuración, operación y administración de un sistema de seguridad de red proactivo Anti-Hacker (Párrafo 0040 del documento D5).

- Reivindicación 12: Además, a medida que se implementan formatos de registro de flujo de red nuevos o modificados, el módulo de gestión de recolección de flujo de red (1115) se puede actualizar en consecuencia (Párrafo 0080 del documento D3). El usuario puede editar la configuración en bruto en la interfaz de usuario. Los cambios se transmiten al dispositivo a través del canal del dispositivo. Una vez que se han actualizado las configuraciones del dispositivo, el usuario puede volver a ejecutar un análisis de las diversas rutas de la red (10) para determinar qué cambio o cambios en las políticas efectivas de la red (Columna 6, Líneas 56 a 61 del documento D4).

La estructura de una GUI segura optimizada es de naturaleza dinámica, basada en los módulos, las opciones y los complementos de INFOSEC que se cargan en el sistema. Las funciones incluyen acceso rápido al motor de actualización de vulnerabilidades y exposiciones dinámicas para seleccionar cuándo, si alguna vez, programar las actualizaciones del sistema, el motor de mapeo dinámico de la red para iniciar un análisis y revisión automatizados de los sistemas operativos, hardware y software conectados a la red basada computadora (Párrafo 0040 del documento D5).

- Reivindicación 13: Finalmente, el programa de análisis de seguridad (14) incluye un administrador de trabajos (96), que interactúa con el módulo de interfaz de usuario (40) y el simulador de red (56). El administrador de trabajos (96) incluye un notificador de alerta (98) y un planificador de trabajos (100). En aquellas realizaciones en las que el programa de análisis de seguridad (14) funciona como un servidor en una disposición cliente-servidor, el administrador de trabajos (96) facilita la programación y ejecución de los procesos de análisis desatendido. El programador de trabajos (100) programa los trabajos y el notificador de alertas (98) genera alertas sobre el estado de los trabajos (Columna 5, Líneas 13 a 22 del documento D4).

El panel de control administrativo proporciona acceso y control de operaciones avanzadas de alerta, como alertas a través de correo electrónico o módulo de buscapersonas en XML, Really Simple Syndication (RSS) o fuentes de noticias HTML para alertas de vulnerabilidad como BUGTRAQ u otra vulnerabilidad de fuente abierta y amenaza de hackers noticiario (Párrafo 0063 del documento D5). La interfaz de la aplicación (152) también admite una interfaz gráfica de usuario ("GUI") en las computadoras cliente (156) o se proporciona a través del software

**REPÚBLICA DE COLOMBIA
SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO**

Oficio N° 12997

Ref. Expediente N° NC2017/0003261

cliente, lo que permite a los usuarios de las computadoras cliente o software cliente realizar la edición de reglas, configurar informes programados y alertas, para realizar análisis interactivos, edición y navegación del modelo de red, vulnerabilidades y resultados de análisis, para ver el estado de seguridad de la red, para realizar la administración de usuarios, para realizar la administración de tareas, para realizar la administración de agentes y para realizar otras Actividades en comunicación con el software del servidor. En algunas realizaciones, la GUI del cliente está codificada por colores según los riesgos presentados por las vulnerabilidades detectadas (Párrafo 0064 del documento D6).

- Reivindicación 14: Los resultados se almacenan y se comparan con cada lista de activos basada en la red que se procesa previamente en formato de texto ASCII para su almacenamiento en un archivo de texto simple, archivo de valores separados por comas (CSV), archivos de lenguaje de marcado extensible (XML) y lenguaje de consultas estructuradas (SQL) tabla de base de datos (Párrafo 0051 del documento D5).

La interfaz de usuario de la reivindicación 24, en la que la interfaz de usuario integra la administración de un sistema de prevención de intrusiones, el análisis del comportamiento de la red y la evaluación de la vulnerabilidad (Reivindicación 17 del documento D5).

Al comparar las vulnerabilidades en bruto con la información sobre la topología de la red y los servicios de red, el sistema combina las vulnerabilidades con la lógica para determinar las vulnerabilidades reales que podrían ser explotadas por un atacante, paso (110) (Párrafo 0029 del documento D6).

El sistema utiliza este modelo de topología de las vulnerabilidades reales y la información correspondiente de la red y los servicios para detectar y analizar los riesgos planteados por los atacantes (Párrafo 0030 del documento D6).

- Reivindicación 15: El método de la reivindicación 7, en el que: la política de ruta de seguridad es una política de comunicación entre nodos y comprende un conjunto de múltiples tuplas, en el que cada tupla comprende una pluralidad de elementos; un número de niveles en el árbol jerárquico corresponde a un número de elementos en una tupla; cada elemento de árbol en un nivel dado se corresponde con un valor único del elemento dentro de la tupla; y el usuario puede modificar una relación entre el orden jerárquico del árbol y el orden de los elementos de la tupla; el paso que representa gráficamente comprende mostrar el árbol jerárquico con ramas que se pueden expandir o contraer, el árbol; y la etapa de recepción comprende recibir una selección de usuario de un criterio de la pluralidad que se debe promover o degradar (Reivindicación 11 del documento D4).

REPÚBLICA DE COLOMBIA
SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO

Oficio N° 12997

Ref. Expediente N° NC2017/0003261

Un sistema para la seguridad de la red, que comprende: un motor de mapeo dinámico que monitorea los activos en una red y detecta cuando un activo se agrega o se elimina de la red, el motor de mapeo dinámico proporciona datos de identificación de activos; una puerta de enlace entre uno o más de los activos y la red; una interfaz para administrar una política relacionada con el uso de la red a través de la puerta de enlace; y un motor de comunicación de contramedidas administrado a través de la interfaz, el motor de comunicación de contramedidas que responde a la política para controlar una o más contramedidas con referencia a una pluralidad de vulnerabilidades (Reivindicación 8 del documento D5).

Las rutas de acción representan rutas a través de la red que se pueden tomar para realizar ciertas acciones. Una ruta de acción puede ser una acción legítima y cumplir con una política de seguridad como leer páginas web desde servidores web o una ruta de acción puede violar una política de seguridad como leer registros de servidor web para obtener números de tarjetas de crédito (Párrafo 0031 del documento D6).

Las reivindicaciones dependientes 2 a 15 no mencionan alguna característica que haga nuevo al método de la reivindicación 1, por lo cual se considera que no son nuevas.

La reivindicación 16 consiste en: *“Un medio legible por computadora no transitorio, tangible (814), caracterizado porque almacena instrucciones que, cuando se ejecutan, provocan que un sistema de computadora (800) (...)”* (Radicado NC2017/0003261 del 6 de agosto de 2018).

Comparación de las características esenciales con el estado de la técnica.

Características esenciales	D3	D4
Un medio legible por computadora no transitorio, tangible (814), caracterizado porque almacena instrucciones que, cuando se ejecutan, provocan que un sistema de computadora (800).	El método incluye una operación (1801) para adquirir datos de configuración de dispositivos de una serie de dispositivos de red a través de los cuales se transmitirán los flujos de red. En una realización, se genera una tabla de información del dispositivo para incluir los datos de configuración del dispositivo adquiridos, y la tabla de información del dispositivo se almacena en un medio de almacenamiento legible por computadora (Párrafo 0102).	El visor de informes (52) muestra informes que contienen información sobre la seguridad de la red (10). El módulo de interfaz de usuario (40) interactúa con un administrador de repositorio (54) y un simulador de red (56) (Columna 3, Líneas 41 a 45).

Página 21 de 36

**REPÚBLICA DE COLOMBIA
SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO**

Oficio N° 12997

Ref. Expediente N° NC2017/0003261

Recolecte datos (905) de una pluralidad de diferentes tipos de fuentes, en donde los datos recolectados incluyen datos de la red y datos de recursos.	La correlación de los flujos de red de dispositivo a dispositivo requiere algún almacenamiento de datos de flujo de red, ya que la llegada de datos de flujo de red al módulo de correlación (1119) de diferentes dispositivos puede variar en el tiempo, dependiendo de las técnicas utilizadas para recopilar el flujo de red datos. Además, es posible que se requiera el almacenamiento en caché de los datos de flujo de la red para evitar la pérdida prematura de los datos de flujo de la red antes de que se puedan representar visualmente en la GUI (1300) (Párrafo 0090).	En algún momento, antes o después de que el usuario inicie el programa de análisis de seguridad (14), los adaptadores de dispositivo (90), (92) y (94) recuperan la información de configuración de sus dispositivos respectivos (91), (93) y (95). Los ejemplos de información de configuración recopilada incluyen reglas de control de acceso, reglas de autenticación y reglas para verificar la integridad de los datos. El adaptador de dispositivo puede obtener este tipo de datos en forma de reglas de firewall almacenadas en el dispositivo con el que está asociado (Columna 5, Líneas 23 a 30).
Identifique (915), 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 relacionados con el evento del tráfico de la red.	El método también incluye una operación (1803) para analizar los datos de configuración del dispositivo adquiridos para identificar una o más interfaces de cada número de dispositivos de red, y para identificar subredes a las que se conectan una o más interfaces (Párrafo 0102).	Hay muchas formas posibles de generar la información de topología contenida en la base de datos de topologías (58). En una realización, la topología se crea a través de un proceso manual, en el que el usuario identifica todos los segmentos de red y dispositivos que se utilizarán en la topología. El usuario también crea una definición de red o host para cada elemento de la topología. El usuario coloca cada red o dispositivo en el diagrama de topología (Columna 4, Líneas 14 a 21).
Identifique (920), con base en los datos de recursos en los datos recolectados, conexiones entre la pluralidad de recursos de la red, en el que una de las características de una conexión entre recursos de red o una característica de un recurso de red se identifica con base en un atributo seleccionado de los datos recolectados.	Los segmentos de línea representan conexiones de red a través de las cuales se transmitirán los flujos de red. Además, en una realización, se realiza una operación para representar en la visualización visual una vista jerárquica del número de dispositivos de red y las interfaces dentro del número de dispositivos de red. También en esta realización, tras la selección de un dispositivo de red particular en la vista jerárquica, se representa una vista aislada del dispositivo de red seleccionado particular en la pantalla visual (Párrafo 0104).	El programa de análisis de seguridad (14) luego determina la naturaleza de las conexiones entre redes y dispositivos basándose en parte en los rangos de direcciones de red de las redes y las direcciones de Protocolo de Internet (IP) de las interfaces de red asociadas con los dispositivos. En otra realización, el programa de análisis de seguridad (14) descubre automáticamente la topología utilizando una herramienta de descubrimiento de topología convencional y varias herramientas de gestión de red (Columna 4, Líneas 22 a 30).
En respuesta a la detección, basada en los datos recolectados (905),	La GUI (1300) incluye una primera región de visualización (1303) dentro de la cual se representa visualmente	La red de computadoras, generalmente etiquetada (10) incluye una computadora (12) en la que se

REPÚBLICA DE COLOMBIA
SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO

Oficio N° 12997

Ref. Expediente N° NC2017/0003261

un cambio en un atributo (420) de un primer recurso de red asociado con una primera zona lógica, moviendo (430) el primer recurso de red de la primera zona lógica a una segunda zona lógica, el movimiento comprende actualizar una base de datos para indicar que el primer recurso de red es un miembro de la segunda zona lógica, y en base a la membresía en la segunda zona lógica, la comunicación entre el primer recurso de red y otros recursos de red está bloqueada.	la visualización de la topología de la red (1113). Los dispositivos de red (1104A) - (1104C) se muestran como círculos grandes (Párrafo 0076).	ejecuta el programa de análisis de seguridad (14). La red de computadoras (10) también incluye las puertas de enlace primera y segunda (16) y (18), y tres "hosts significativos" (20), (22) y (24). Tal como se usa en el presente documento, el término "host significativo" significa cualquier host que almacene valiosos activos de información o ejecute software que sea crítico para el funcionamiento del negocio de la entidad que utiliza la red (10) (incluidos comerciales, públicos / gubernamentales o no - entidades lucrativas) (Columna 3, líneas 12 a 20).
Genere una gráfica de información de flujo (925) que representa la pluralidad de recursos de la red y las conexiones entre la pluralidad de recursos de la red, en donde la pluralidad de recursos de red incluye el primer recurso de red y la información de flujo del gráfico representa el tráfico de red permitido entre los recursos de la red y el tráfico de la red que está bloqueado entre los recursos de la red.	El módulo de visualización de red se define además para representar en una pantalla visual una vista de topología de la red que incluye representaciones gráficas de los dispositivos, interfaces dentro de los dispositivos y conexiones entre las interfaces y las subredes. El sistema también incluye un módulo de gestión de recolección de flujo de red definido para adquirir registros de flujo de red de cada dispositivo dentro de la red (Párrafo 0006).	Un método para analizar la seguridad de una red informática, que comprende: recopilar los ajustes de configuración de seguridad de cada uno de una pluralidad de nodos de la red informática, para cada nodo: abrir una sesión de comunicación con el nodo, consultar el nodo utilizando la sesión de comunicación para determinar las configuraciones de configuración de seguridad del nodo; y obtener reglas que cada uno de los nodos utiliza para admitir o denegar el tráfico de red; mostrar gráficamente la topología de la red en una interfaz de usuario al mostrar una representación para cada uno de los nodos en la red y mostrar las conexiones entre las representaciones, las conexiones son representativas de las rutas de comunicación entre cada uno de los nodos (Reivindicación 1).
Presente la gráfica de información de flujo (930) a través de la pantalla de una interfaz de usuario en comunicación con el sistema de computadora, en el que el gráfico de información de flujo	El módulo de visualización de red (1109) se define además para representar en una pantalla visual de un sistema informático, una visualización de topología de red (1113) que incluye una vista de topología de la red (1102), que incluye representaciones gráficas de los	El método de la reivindicación 1, en el que el paso de visualización gráfica comprende visualizar un icono como la representación de cada uno de los nodos en la red y visualizar líneas como las conexiones entre los iconos, siendo las líneas representativas de

**REPÚBLICA DE COLOMBIA
SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO**

Oficio N° 12997

Ref. Expediente N° NC2017/0003261

representa conexiones entre los recursos de red usando líneas de flujo direccional seleccionables.	dispositivos (1104), las interfaces (1101) dentro de los dispositivos (1101), y varias conexiones entre las interfaces (1101) y las subredes. Las interfaces lógicas, como el bucle de retorno del enrutador, la interfaz nula, la interfaz local, la interfaz VLAN, los túneles, etc., también se muestran en la visualización de la topología de la red (1113) (Párrafo 0075).	las rutas de comunicación entre los nodos (Reivindicación 4).
Y en respuesta a la selección (935), por un usuario a través de la interfaz de usuario, de una línea de flujo respectiva asociada a una conexión desde la pluralidad de conexiones, mostrar las características de la conexión seleccionada (940) incluyendo reglas de visualización para permitir y bloquear el tráfico sobre la conexión seleccionada.	Un usuario puede seleccionar el dispositivo particular (1609) dentro de la vista jerárquica de la red dentro de la segunda región de pantalla (1305). Una vista aislada del dispositivo seleccionado (1609) se representa en la primera región de pantalla (1303) que muestra el dispositivo (1609) junto con sus interfaces y flechas que representan los diversos flujos de red asociados con el dispositivo (1609) (Párrafo 0092).	En el que el dispositivo de interfaz de usuario comprende un módulo de interfaz de usuario que realiza pasos que comprenden: recibir una selección de usuario del primer dispositivo y del segundo dispositivo; mostrar, para el usuario, la política de ruta de seguridad derivada en forma de árbol, el árbol está estructurado según el orden de clasificación de los criterios; recibir, del usuario, una solicitud para cambiar el orden de clasificación de los criterios; y volver a mostrar el árbol al usuario en función del orden de clasificación modificado (Reivindicación 12).

Adicionalmente los documentos D5 y D6 divulgan las características esenciales de la invención a continuación:

Comparación de las características esenciales con el estado de la técnica para la reivindicación.

Características esenciales	D5	D6
Un medio legible por computadora no transitorio, tangible (814), caracterizado porque almacena instrucciones que, cuando se ejecutan, provocan que un sistema de computadora (800).	El método proporciona acceso GUI basado en web seguro a estos informes al leer dinámicamente una lista de todos los resultados de pruebas CVE disponibles y sus informes relacionados en una lista de selección simple con una interfaz de apuntar y hacer clic para que los administradores autorizados puedan acceder a ellos (Párrafo 0052).	Como se muestra, el sistema incluye una computadora servidor (141) que incluye software de servidor, que incluye un módulo de la unidad de control (142), un módulo del gestor de recopilación (144), un módulo de motor analítico (146), un módulo generador de alertas (148), un módulo de generación de informes (150), un módulo de interfaz de aplicación (152) y un módulo de actualización de cliente (154) (Párrafo 0057).

**REPÚBLICA DE COLOMBIA
SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO**

Oficio N° 12997

Ref. Expediente N° NC2017/0003261

Recolecte datos (905) de una pluralidad de diferentes tipos de fuentes, en donde los datos recolectados incluyen datos de la red y datos de recursos.	En funcionamiento, el hardware está conectado a una red basada en computadora a través de los medios estándar de conectividad que incluyen, entre otros, una conexión TCP / IP por cable o inalámbrica. A continuación, el administrador lo configura rápidamente a través de la GUI segura. Una vez configurado, el sistema puede explorar opcionalmente la red de acceso local para determinar la topología de la red y recopilar información sobre el sistema operativo y la dirección IP (Párrafo 0050).	De acuerdo con algunos aspectos de la presente invención, se proporcionan métodos para realizar una evaluación de vulnerabilidad automatizada en una red de computadoras, los métodos que involucran la recopilación de información sobre la red y sus componentes, creando un modelo de la red (que puede incluir todos sus nodos y sus configuraciones / servicios), simulando posibles ataques contra la red utilizando gráficos de ataques, generando las consecuencias correspondientes de posibles ataques, calculando la probabilidad de que ocurran ataques y clasificando las vulnerabilidades asociadas con posibles ataques (Párrafo 0012).
Identifique (915), 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 relacionados con el evento del tráfico de la red.	El método de la reivindicación 12, en el que la lista de activos identifica puertos abiertos para cada uno de los uno o más activos (Reivindicación 5).	El algoritmo puede primero identificar o seleccionar nodos de puntos de inicio para los ataques. El algoritmo puede utilizar la información de restricción asociada con los nodos del gráfico de conexión para determinar posibles rutas de ataque desde los nodos del gráfico de punto de inicio a través de otros nodos del gráfico de conexión, y para determinar los nodos del gráfico de punto de terminación del ataque (Párrafo 0013).
Identifique (920), con base en los datos de recursos en los datos recolectados, conexiones entre la pluralidad de recursos de la red, en el que una de las características de una conexión entre recursos de red o una característica de un recurso de red se identifica con base en un atributo seleccionado de los datos recolectados.	El método de la reivindicación 12, en el que para cada uno de los uno o más activos, la lista identifica una o más de una dirección de control de acceso a medios, información de aplicación, información de sesión, información de transporte, información de socket y un tipo de conexión (Reivindicación 6).	Los agentes de descubrimiento (158) recopilan información de red con respecto a vulnerabilidades sin formato, topología, servicios y otra información. Los agentes de descubrimiento ejemplares (158) incluyen agentes de firewall, agentes de topología de red, agentes de servicio, agentes de escáner de vulnerabilidad en bruto y otros agentes. Los agentes especializados recopilan información específica de nodos de red específicos. Por ejemplo, los agentes de firewall, por ejemplo, recopilan listas de control de acceso y conjuntos de reglas de filtrado; Los agentes de topología de red recopilan información sobre las

**REPÚBLICA DE COLOMBIA
SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO**

Oficio N° 12997

Ref. Expediente N° NC2017/0003261

		interconexiones entre los dispositivos de red y los hosts (Párrafo 0060).
En respuesta a la detección, basada en los datos recolectados (905), un cambio en un atributo (420) de un primer recurso de red asociado con una primera zona lógica, moviendo (430) el primer recurso de red de la primera zona lógica a una segunda zona lógica, el movimiento comprende actualizar una base de datos para indicar que el primer recurso de red es un miembro de la segunda zona lógica, y en base a la membresía en la segunda zona lógica, la comunicación entre el primer recurso de red y otros recursos de red está bloqueada.	En el caso de que la contramedida de INFOSEC sea un IPS, una alerta dinámica del administrador de TI o un destinatario de alerta alternativo y se realizarán cambios dinámicos en la lista de acceso a IPS a través del complemento del cliente de comunicaciones de contramedidas que se ha escrito específicamente para ese MAKE, MODELO y VERSION IPS. En el caso de que la contramedida de INFOSEC sea un IDS, una alerta dinámica del administrador de TI o un receptor de alerta alternativo y compartir los datos de pruebas CVE relacionados con el IDS para ayudar al IDS a reducir los falsos positivos en el módulo de alerta del IDS, así como a reducir la carga de tráfico. relacionado con las detecciones de intrusión que atacan una dirección IP particular que no es susceptible a esa metodología de ataque particular basada en los datos de pruebas CVE relacionados y se llevará a cabo a través del complemento de cliente de comunicaciones de contramedidas que se ha escrito específicamente para ese MAKE, MODELO y VERSIÓN IDS (Párrafo 0057).	Se envían paquetes de datos a cada dispositivo de red y se interpretan las respuestas recibidas de los dispositivos de red para determinar si existe una vulnerabilidad sin formato. Por ejemplo, un agente de descubrimiento de información podría realizar pruebas para determinar si una versión particular de BIND vulnerable a los ataques está presente. El agente de descubrimiento de información enviaría paquetes que contengan un comando de consulta para que el servidor BIND en una red devuelva su número de versión (Párrafo 0067).
Genere una gráfica de información de flujo (925) que representa la pluralidad de recursos de la red y las conexiones entre la pluralidad de recursos de la red, en donde la pluralidad de recursos de red incluye el primer recurso de red y la información de flujo del gráfico representa el tráfico	Volviendo ahora de forma descriptiva a los dibujos, en los que los caracteres de referencia similares denotan elementos similares en las distintas vistas, las figuras adjuntas ilustran un sistema de seguridad de red proactivo para protegerse contra piratas informáticos, que comprende una interfaz gráfica de usuario (GUI) de factores humanos en diseño (HFID) para la configuración y administración seguras (Párrafo 0039).	El método de la reivindicación 44, en el que generar un gráfico de ataque usando un algoritmo de línea frontal móvil comprende: seleccionar uno o más primeros nodos de gráfico; determinar, para un segundo nodo gráfico, si las restricciones en el estado de servicio asociado con el segundo nodo gráfico están satisfechas por el estado de uno o más primeros nodos gráficos; y agregar un borde que conecta uno o más primeros nodos de gráfico al segundo nodo de gráfico si las restricciones en el estado de servicio asociado con el segundo nodo de gráfico se satisfacen con el estado de uno o más primeros nodos de gráfico (Reivindicación 18).
		El método de la reivindicación 29, en el que generar un gráfico de ataque comprende usar un algoritmo de primera línea móvil (Reivindicación 17).

REPÚBLICA DE COLOMBIA
SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO

Oficio N° 12997

Ref. Expediente N° NC2017/0003261

de red permitido entre los recursos de la red y el tráfico de la red que está bloqueado entre los recursos de la red.		
Presente la gráfica de información de flujo (930) a través de la pantalla de una interfaz de usuario en comunicación con el sistema de computadora, en el que el gráfico de información de flujo representa conexiones entre los recursos de red usando líneas de flujo direccional seleccionables.	Una vez que haya iniciado sesión en la GUI segura, un administrador puede navegar rápida y fácilmente a través de los botones gráficos y el texto del hipervínculo. La navegación está optimizada para los medios más rápidos de configuración, operación y administración de un sistema de seguridad de red proactivo Anti-Hacker (Párrafo 0040).	El método de la reivindicación 44, en el que generar un gráfico de ataque usando un algoritmo de línea frontal móvil comprende: seleccionar uno o más primeros nodos de gráfico; determinar, para un segundo nodo gráfico, si las restricciones en el estado de servicio asociado con el segundo nodo gráfico están satisfechas por el estado de uno o más primeros nodos gráficos; y agregar un borde que conecta uno o más primeros nodos de gráfico al segundo nodo de gráfico si las restricciones en el estado de servicio asociado con el segundo nodo de gráfico se satisfacen con el estado de uno o más primeros nodos de gráfico (Reivindicación 18).
Y en respuesta a la selección (935), por un usuario a través de la interfaz de usuario, de una línea de flujo respectiva asociada a una conexión desde la pluralidad de conexiones, mostrar las características de la conexión seleccionada (940) incluyendo reglas de visualización para permitir y bloquear el tráfico sobre la conexión seleccionada.	El panel de control administrativo proporciona acceso y control de operaciones avanzadas de alerta, como alertas a través del correo electrónico o módulo de buscapersonas al finalizar el descubrimiento de activos basado en la red. El panel de control administrativo proporciona acceso y control de operaciones avanzadas de alerta, como alertas a través de correo electrónico o módulo de buscapersonas al finalizar la prueba CVE en uno o más activos seleccionados de la red en una base por dirección IP (Párrafo 0063).	

De acuerdo con las dos tablas anteriores, las características esenciales del medio legible de la reivindicación 16 habían sido divulgadas previamente en los documentos D3 a D6, por lo tanto, la materia reivindicada no es nueva.

La reivindicación 17 consiste en: *“Un sistema de computadora (800), caracterizado porque comprende: un procesador (812); y memoria (814) en comunicación con el procesador y las instrucciones de almacenamiento que, cuando se ejecutan por el procesador, provocan que el sistema de computadora (...)”* (Radicado NC2017/0003261 del 6 de agosto de 2018).

REPÚBLICA DE COLOMBIA
SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO

Oficio N° 12997

Ref. Expediente N° NC2017/0003261

Comparación de las características esenciales con el estado de la técnica.

Características esenciales	D3	D4
Un sistema de computadora (800), caracterizado porque comprende: un procesador (812); y memoria (814) en comunicación con el procesador y las instrucciones de almacenamiento que, cuando se ejecutan por el procesador, provocan que el sistema de computadora (...)	En varias formas de realización, la herramienta de monitoreo de red (209) se puede definir para registrar métricas del dispositivo, como el uso de la CPU, el uso de la memoria, la tasa de política previa, la tasa de política posterior, la profundidad de la cola, la caída de paquetes, entre otros. Además de las métricas de dispositivo específicas identificadas anteriormente, debe entenderse que la herramienta de monitoreo de red (209) se puede definir para determinar esencialmente cualquier otro tipo de métrica de dispositivo (Párrafo 0040).	Aquí se describe un método y un sistema para analizar la seguridad de una red de computadoras. De acuerdo con varias implementaciones, hay un adaptador de dispositivo asociado con cada dispositivo que tiene un impacto significativo en la seguridad de la red (por ejemplo, enrutadores, conmutadores, puertas de enlace o "hosts significativos"). El adaptador del dispositivo, que puede implementarse como una pieza de software que se ejecuta de forma remota desde el dispositivo, consulta al dispositivo para determinar cuáles son sus configuraciones de seguridad (por ejemplo, sus reglas de firewall) (Resumen).
Recolecte datos (905) de una pluralidad de diferentes tipos de fuentes, en donde los datos recolectados incluyen datos de la red y datos de recursos.	La correlación de los flujos de red de dispositivo a dispositivo requiere algún almacenamiento de datos de flujo de red, ya que la llegada de datos de flujo de red al módulo de correlación (1119) de diferentes dispositivos puede variar en el tiempo, dependiendo de las técnicas utilizadas para recopilar el flujo de red datos. Además, es posible que se requiera el almacenamiento en caché de los datos de flujo de la red para evitar la pérdida prematura de los datos de flujo de la red antes de que se puedan representar visualmente en la GUI (1300) (Párrafo 0090).	En algún momento, antes o después de que el usuario inicie el programa de análisis de seguridad (14), los adaptadores de dispositivo (90), (92) y (94) recuperan la información de configuración de sus dispositivos respectivos (91), (93) y (95). Los ejemplos de información de configuración recopilada incluyen reglas de control de acceso, reglas de autenticación y reglas para verificar la integridad de los datos. El adaptador de dispositivo puede obtener este tipo de datos en forma de reglas de firewall almacenadas en el dispositivo con el que está asociado (Columna 5, Líneas 23 a 30).
Identifique (915), 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 relacionados con el evento de tráfico de la red.	El método también incluye una operación (1803) para analizar los datos de configuración del dispositivo adquiridos para identificar una o más interfaces de cada número de dispositivos de red, y para identificar subredes a las que se conectan una o más interfaces (Párrafo 0102).	Hay muchas formas posibles de generar la información de topología contenida en la base de datos de topologías (58). En una realización, la topología se crea a través de un proceso manual, en el que el usuario identifica todos los segmentos de red y dispositivos que se utilizarán en la topología. El usuario también crea una definición de red o host para cada elemento de la topología. El usuario

REPÚBLICA DE COLOMBIA
SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO

Oficio N° 12997

Ref. Expediente N° NC2017/0003261

		coloca cada red o dispositivo en el diagrama de topología (Columna 4, Líneas 14 a 21).
Identifique (920), con base en los datos de recursos en los datos recolectados, conexiones entre la pluralidad de recursos de la red, en el que una de las características de una conexión entre recursos de red o una característica de un recurso de red se identifica con base en un atributo seleccionado de los datos recolectados.	Los segmentos de línea representan conexiones de red a través de las cuales se transmitirán los flujos de red. Además, en una realización, se realiza una operación para representar en la visualización visual una vista jerárquica del número de dispositivos de red y las interfaces dentro del número de dispositivos de red. También en esta realización, tras la selección de un dispositivo de red particular en la vista jerárquica, se representa una vista aislada del dispositivo de red seleccionado particular en la pantalla visual (Párrafo 0104).	El programa de análisis de seguridad (14) luego determina la naturaleza de las conexiones entre redes y dispositivos basándose en parte en los rangos de direcciones de red de las redes y las direcciones de Protocolo de Internet (IP) de las interfaces de red asociadas con los dispositivos. En otra realización, el programa de análisis de seguridad (14) descubre automáticamente la topología utilizando una herramienta de descubrimiento de topología convencional y varias herramientas de gestión de red (Columna 4, Líneas 22 a 30).
En respuesta a detectar, basado en los datos recolectados (905), un cambio en un atributo (420) de un primer recurso de red asociado con una primera zona lógica, moviendo (430) el primer recurso de red de la primera zona lógica a una segunda zona lógica, el movimiento comprende actualizar una base de datos para indicar que el primer recurso de red es un miembro de la segunda zona lógica, y en base a la membresía en la segunda zona lógica, la comunicación entre el primer recurso de red y otros recursos de red está bloqueada.	La GUI (1300) incluye una primera región de visualización (1303) dentro de la cual se representa visualmente la visualización de la topología de la red (1113). Los dispositivos de red (1104A) - (1104C) se muestran como círculos grandes (Párrafo 0076).	La red de computadoras, generalmente etiquetada (10) incluye una computadora (12) en la que se ejecuta el programa de análisis de seguridad (14). La red de computadoras (10) también incluye las puertas de enlace primera y segunda (16) y (18), y tres "hosts significativos" (20), (22) y (24). Tal como se usa en el presente documento, el término "host significativo" significa cualquier host que almacene valiosos activos de información o ejecute software que sea crítico para el funcionamiento del negocio de la entidad que utiliza la red (10) (incluidos comerciales, públicos / gubernamentales o no - entidades lucrativas) (Columna 3, líneas 12 a 20).
Genere una gráfica de información de flujo (925) que representa la pluralidad de recursos de la red y las conexiones entre la pluralidad de recursos de la red, en donde la pluralidad de recursos de red incluye el primer	El módulo de visualización de red se define además para representar en una pantalla visual una vista de topología de la red que incluye representaciones gráficas de los dispositivos, interfaces dentro de los dispositivos y conexiones entre las interfaces y las subredes. El sistema también incluye un módulo de gestión	Un método para analizar la seguridad de una red informática, que comprende: recopilar los ajustes de configuración de seguridad de cada uno de una pluralidad de nodos de la red informática, para cada nodo: abrir una sesión de comunicación con el nodo, consultar el nodo utilizando la sesión de comunicación para

REPÚBLICA DE COLOMBIA
SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO

Oficio N° 12997

Ref. Expediente N° NC2017/0003261

recurso de red y la información de flujo del gráfico representa el tráfico de red permitido entre los recursos de la red y el tráfico de la red que está bloqueado entre los recursos de la red.	de recolección de flujo de red definido para adquirir registros de flujo de red de cada dispositivo dentro de la red (Párrafo 0006).	determinar las configuraciones de configuración de seguridad del nodo; y obtener reglas que cada uno de los nodos utiliza para admitir o denegar el tráfico de red; mostrar gráficamente la topología de la red en una interfaz de usuario al mostrar una representación para cada uno de los nodos en la red y mostrar las conexiones entre las representaciones, las conexiones son representativas de las rutas de comunicación entre cada uno de los nodos (Reivindicación 1).
Y presente la gráfica de información de flujo (930) a través de una pantalla de una interfaz de usuario en comunicación con el sistema de computadora, en el que el gráfico de información de flujo representa conexiones entre los recursos de red usando líneas de flujo direccional seleccionables.	El módulo de visualización de red (1109) se define además para representar en una pantalla visual de un sistema informático, una visualización de topología de red (1113) que incluye una vista de topología de la red (1102), que incluye representaciones gráficas de los dispositivos (1104), las interfaces (1101) dentro de los dispositivos (1101), y varias conexiones entre las interfaces (1101) y las subredes. Las interfaces lógicas, como el bucle de retorno del enrutador, la interfaz nula, la interfaz local, la interfaz VLAN, los túneles, etc., también se muestran en la visualización de la topología de la red (1113) (Párrafo 0075).	El método de la reivindicación 1, en el que el paso de visualización gráfica comprende visualizar un icono como la representación de cada uno de los nodos en la red y visualizar líneas como las conexiones entre los iconos, siendo las líneas representativas de las rutas de comunicación entre los nodos (Reivindicación 4).
Y en respuesta a la selección (935), por un usuario a través de la interfaz de usuario, de una línea de flujo respectiva asociada a una conexión desde la pluralidad de conexiones, mostrar las características de la conexión seleccionada (940) incluyendo reglas de visualización para permitir y bloquear el tráfico sobre la conexión seleccionada.	Un usuario puede seleccionar el dispositivo particular (1609) dentro de la vista jerárquica de la red dentro de la segunda región de pantalla (1305). Una vista aislada del dispositivo seleccionado (1609) se representa en la primera región de pantalla (1303) que muestra el dispositivo (1609) junto con sus interfaces y flechas que representan los diversos flujos de red asociados con el dispositivo (1609) (Párrafo 0092).	En el que el dispositivo de interfaz de usuario comprende un módulo de interfaz de usuario que realiza pasos que comprenden: recibir una selección de usuario del primer dispositivo y del segundo dispositivo; mostrar, para el usuario, la política de ruta de seguridad derivada en forma de árbol, el árbol está estructurado según el orden de clasificación de los criterios; recibir, del usuario, una solicitud para cambiar el orden de clasificación de los criterios; y volver a mostrar el árbol al usuario en función del orden de clasificación modificado (Reivindicación 12).

REPÚBLICA DE COLOMBIA
SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO

Oficio N° 12997

Ref. Expediente N° NC2017/0003261

Adicionalmente los documentos D5 y D6 divulgan las características esenciales de la invención a continuación:

Comparación de las características esenciales con el estado de la técnica.

Características esenciales	D5	D6
Un sistema de computadora (800), caracterizado porque comprende: un procesador (812); y memoria (814) en comunicación con el procesador y las instrucciones de almacenamiento que, cuando se ejecutan por el procesador, provocan que el sistema de computadora (...)	Otro objetivo es proporcionar un sistema de seguridad de red proactivo para protegerse contra los piratas informáticos que contiene una CPU, una memoria, un disco duro para el almacenamiento que todos pueden actualizarse fácilmente con soluciones de "caja abierta" listas para usa (Párrafo 0017).	Los resultados de la simulación de ataque se almacenan en la memoria y se utilizan para generar una lista de posibles ataques en la red, paso (125). Una vez que se genera la lista de posibles ataques, el sistema calcula las consecuencias correspondientes de cada posible ataque, paso (130) (Párrafo 0052). Como se muestra, el sistema incluye una computadora servidor (141) que incluye software de servidor, que incluye un módulo de la unidad de control (142), un módulo del gestor de recopilación (144), un módulo de motor analítico (146), un módulo generador de alertas (148), un módulo de generación de informes (150), un módulo de interfaz de aplicación (152) y un módulo de actualización de cliente (154) (Párrafo 0058).
Recolecte datos (905) de una pluralidad de diferentes tipos de fuentes, en donde los datos recolectados incluyen datos de la red y datos de recursos.	En funcionamiento, el hardware está conectado a una red basada en computadora a través de los medios estándar de conectividad que incluyen, entre otros, una conexión TCP / IP por cable o inalámbrica. A continuación, el administrador lo configura rápidamente a través de la GUI segura. Una vez configurado, el sistema puede explorar opcionalmente la red de acceso local para determinar la topología de la red y recopilar información sobre el sistema operativo y la dirección IP (Párrafo 0050).	De acuerdo con algunos aspectos de la presente invención, se proporcionan métodos para realizar una evaluación de vulnerabilidad automatizada en una red de computadoras, los métodos que involucran la recopilación de información sobre la red y sus componentes, creando un modelo de la red (que puede incluir todos sus nodos y sus configuraciones / servicios), simulando posibles ataques contra la red utilizando gráficos de ataques, generando las consecuencias correspondientes de posibles ataques, calculando la probabilidad de que ocurran ataques y clasificando las vulnerabilidades asociadas con posibles ataques (Párrafo 0012).

REPÚBLICA DE COLOMBIA
SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO

Oficio N° 12997

Ref. Expediente N° NC2017/0003261

Identifique (915), 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 relacionados con el evento de tráfico de la red.	El método de la reivindicación 12, en el que la lista de activos identifica puertos abiertos para cada uno de los uno o más activos (Reivindicación 5).	El algoritmo puede primero identificar o seleccionar nodos de puntos de inicio para los ataques. El algoritmo puede utilizar la información de restricción asociada con los nodos del gráfico de conexión para determinar posibles rutas de ataque desde los nodos del gráfico de punto de inicio a través de otros nodos del gráfico de conexión, y para determinar los nodos del gráfico de punto de terminación del ataque (Párrafo 0013).
Identifique (920), con base en los datos de recursos en los datos recolectados, conexiones entre la pluralidad de recursos de la red, en el que una de las características de una conexión entre recursos de red o una característica de un recurso de red se identifica con base en un atributo seleccionado de los datos recolectados.	El método de la reivindicación 12, en el que para cada uno de los uno o más activos, la lista identifica una o más de una dirección de control de acceso a medios, información de aplicación, información de sesión, información de transporte, información de socket y un tipo de conexión (Reivindicación 6).	Los agentes de descubrimiento (158) recopilan información de red con respecto a vulnerabilidades sin formato, topología, servicios y otra información. Los agentes de descubrimiento ejemplares (158) incluyen agentes de firewall, agentes de topología de red, agentes de servicio, agentes de escáner de vulnerabilidad en bruto y otros agentes. Los agentes especializados recopilan información específica de nodos de red específicos. Por ejemplo, los agentes de firewall, por ejemplo, recopilan listas de control de acceso y conjuntos de reglas de filtrado; Los agentes de topología de red recopilan información sobre las interconexiones entre los dispositivos de red y los hosts (Párrafo 0060).
En respuesta a detectar, basado en los datos recolectados (905), un cambio en un atributo (420) de un primer recurso de red asociado con una primera zona lógica, moviendo (430) el primer recurso de red de la primera zona lógica a una segunda zona lógica, el movimiento comprende actualizar una base de datos para indicar que el primer recurso de red es un miembro de la segunda zona lógica, y en base a la membresía en la	En el caso de que la contramedida de INFOSEC sea un IPS, una alerta dinámica del administrador de TI o un destinatario de alerta alternativo y se realizarán cambios dinámicos en la lista de acceso a IPS a través del complemento del cliente de comunicaciones de contramedidas que se ha escrito específicamente para ese MAKE, MODELO y VERSION IPS. En el caso de que la contramedida de INFOSEC sea un IDS, una alerta dinámica del administrador de TI o un receptor de alerta alternativo y compartir los datos de pruebas CVE relacionados con el IDS para ayudar al IDS a reducir los falsos positivos en el módulo de alerta	Se envían paquetes de datos a cada dispositivo de red y se interpretan las respuestas recibidas de los dispositivos de red para determinar si existe una vulnerabilidad sin formato. Por ejemplo, un agente de descubrimiento de información podría realizar pruebas para determinar si una versión particular de BIND vulnerable a los ataques está presente. El agente de descubrimiento de información enviaría paquetes que contengan un comando de consulta para que el servidor BIND en una red devuelva su número de versión (Párrafo 0067).

REPÚBLICA DE COLOMBIA
SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO

Oficio N° 12997

Ref. Expediente N° NC2017/0003261

segunda zona lógica, la comunicación entre el primer recurso de red y otros recursos de red está bloqueada.	del IDS, así como a reducir la carga de tráfico. relacionado con las detecciones de intrusión que atacan una dirección IP particular que no es susceptible a esa metodología de ataque particular basada en los datos de pruebas CVE relacionados y se llevará a cabo a través del complemento de cliente de comunicaciones de contramedidas que se ha escrito específicamente para ese MAKE, MODELO y VERSIÓN IDS (Párrafo 0057).	El método de la reivindicación 44, en el que generar un gráfico de ataque usando un algoritmo de línea frontal móvil comprende: seleccionar uno o más primeros nodos de gráfico; determinar, para un segundo nodo gráfico, si las restricciones en el estado de servicio asociado con el segundo nodo gráfico están satisfechas por el estado de uno o más primeros nodos gráficos; y agregar un borde que conecta uno o más primeros nodos de gráfico al segundo nodo de gráfico si las restricciones en el estado de servicio asociado con el segundo nodo de gráfico se satisfacen con el estado de uno o más primeros nodos de gráfico (Reivindicación 18).
Genere una gráfica de información de flujo (925) que representa la pluralidad de recursos de la red y las conexiones entre la pluralidad de recursos de la red, en donde la pluralidad de recursos de red incluye el primer recurso de red y la información de flujo del gráfico representa el tráfico de red permitido entre los recursos de la red y el tráfico de la red que está bloqueado entre los recursos de la red.	Volviendo ahora de forma descriptiva a los dibujos, en los que los caracteres de referencia similares denotan elementos similares en las distintas vistas, las figuras adjuntas ilustran un sistema de seguridad de red proactivo para protegerse contra piratas informáticos, que comprende una interfaz gráfica de usuario (GUI) de factores humanos en diseño (HFID) para la configuración y administración seguras (Párrafo 0039).	El método de la reivindicación 29, en el que generar un gráfico de ataque comprende usar un algoritmo de primera línea móvil (Reivindicación 17).
Y presente la gráfica de información de flujo (930) a través de una pantalla de una interfaz de usuario en comunicación con el sistema de computadora, en el que el gráfico de información de flujo representa conexiones entre los recursos de red usando líneas de flujo direccional seleccionables.	Una vez que haya iniciado sesión en la GUI segura, un administrador puede navegar rápida y fácilmente a través de los botones gráficos y el texto del hipervínculo. La navegación está optimizada para los medios más rápidos de configuración, operación y administración de un sistema de seguridad de red proactivo Anti-Hacker (Párrafo 0040).	El método de la reivindicación 44, en el que generar un gráfico de ataque usando un algoritmo de línea frontal móvil comprende: seleccionar uno o más primeros nodos de gráfico; determinar, para un segundo nodo gráfico, si las restricciones en el estado de servicio asociado con el segundo nodo gráfico están satisfechas por el estado de uno o más primeros nodos gráficos; y agregar un borde que conecta uno o más primeros nodos de gráfico al segundo nodo de gráfico si las
Y en respuesta a la selección (935), por un	El panel de control administrativo proporciona acceso y control de	

**REPÚBLICA DE COLOMBIA
SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO**

Oficio N° 12997

Ref. Expediente N° NC2017/0003261

usuario a través de la interfaz de usuario, de una línea de flujo respectiva asociada a una conexión desde la pluralidad de conexiones, mostrar las características de la conexión seleccionada (940) incluyendo reglas de visualización para permitir y bloquear el tráfico sobre la conexión seleccionada.	operaciones avanzadas de alerta, como alertas a través del correo electrónico o módulo de buscapersonas al finalizar el descubrimiento de activos basado en la red. El panel de control administrativo proporciona acceso y control de operaciones avanzadas de alerta, como alertas a través de correo electrónico o módulo de buscapersonas al finalizar la prueba CVE en uno o más activos seleccionados de la red en una base por dirección IP (Párrafo 0063).	restricciones en el estado de servicio asociado con el segundo nodo de gráfico se satisfacen con el estado de uno o más primeros nodos de gráfico (Reivindicación 18).
--	--	--

De acuerdo con las dos tablas anteriores, las características esenciales del sistema de la reivindicación 17 habían sido divulgadas previamente en los documentos D3 a D6, por lo tanto, la materia reivindicada no es nueva.

8. Conclusión

Los requisitos de Patentabilidad de la presente solicitud están afectados así:

Ítem	Documento	Reivindicaciones afectadas	Requisitos que afecta
D3	US2009327903A1	1 a 8, 10 y 11	Novedad
D4	US7849497B1	1 a 6 y 9 a 15	Novedad
D5	US2008005784A1	1 a 8 y 10 a 15	Novedad
D6	US2005193430A1	1 a 4, 8, 9 y 13 a 15	Novedad

9. Respuesta a los argumentos del señor solicitante

Se aceptan las modificaciones presentadas por el solicitante y se procede a ejecutar el examen de fondo.

En cuanto a las objeciones de claridad, se le indica al solicitante que los términos no limitativos u opcionales, crean confusión acerca del alcance de la invención y dificulta diferenciar aquellos elementos diferenciadores del estado de la técnica. En cuanto a los términos de carácter general, se aclara que, aunque se derivan del capítulo descriptivo, pueden dar pie a malinterpretaciones cuando se haga la comparación de la invención con el estado de la técnica.

**REPÚBLICA DE COLOMBIA
SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO**

Oficio N° 12997

Ref. Expediente N° NC2017/0003261

En cuanto al argumento del solicitante: *“Adicionalmente, es importante recordar que un inventor está en su derecho de reclamar protección para la totalidad de un concepto inventivo desarrollado sin importar la amplitud de éste, siempre y cuando se guarde unidad de invención”*, se aclara al solicitante que las sugerencias van orientadas a aclarar el objeto de la invención que se desea proteger, para evitar malinterpretaciones.

El solicitante argumenta que: *“no se pretende reclamar protección sobre la presentación de una gráfica de información de flujo, teniendo en cuenta que la invención se relaciona con un método, sistema y medio legible, sin embargo, hacer referencia a esta es vital para que una persona versada en la materia entienda el funcionamiento y el propósito de dicho método, sistema y medio legible por computador”*, se le aclara al solicitante que la *“presentación de la gráfica”*, es una forma de presentar información ya que según la descripción proporcionada por el solicitante dicha gráfica indica información como: *“la pluralidad de los recursos de la red”, “el tráfico de la red”, “conexiones de los recursos de red”, etc.* Además, el mismo solicitante afirma dentro de la descripción que: *“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”*.

En cumplimiento del artículo 45, de la Decisión 486 de la Comisión de la Comunidad Andina, se le indica que debe dar respuesta dentro del término de sesenta (60) días contados a partir de la fecha de notificación de la presente comunicación. En caso de no dar respuesta al presente requerimiento, o si a pesar de la respuesta subsistieran los impedimentos para la concesión, se denegará la patente.

Si como respuesta a este requerimiento el solicitante llegara a modificar: i) el capítulo reivindicatorio, ii) la descripción de la invención a proteger, iii) o presente un nuevo capítulo reivindicatorio, y desee que se realice un nuevo examen de patentabilidad a esta modificación, no deberá pagar la tasa de modificación voluntaria pero sí la correspondiente a la tasa de examen de patentabilidad. En todo caso, el número de requerimientos por no patentabilidad estará supeditado a que el término del estudio de patentabilidad no sea superior a 18 meses, contados desde la publicación de la solicitud de patente de invención. Adicionalmente, se le recuerda al solicitante que si como respuesta a este requerimiento llegara a modificar el capítulo reivindicatorio y éste contenga más de diez (10) reivindicaciones deberá pagar la tasa por reivindicación adicional.

**REPÚBLICA DE COLOMBIA
SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO**

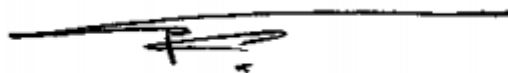
Oficio N° **12997**

Ref. Expediente N° NC2017/0003261

Se invita al solicitante se sirva indicar, si así lo considera, su renuncia al término faltante para los sesenta (60) días.

Notifíquese el presente oficio conforme a lo dispuesto en el numeral 6.2 del Capítulo Sexto del Título I de la Circular Única, informándoles que contra el mismo no procede el recurso de la vía gubernativa.

Atentamente,



**JOSE LUIS SALAZAR LOPEZ
DIRECTOR DE NUEVAS CREACIONES**

Elaborado: DIEGO CAMILO PEÑA RAMÍREZ
Revisado: RACHID PONCE VERJEL