

REPÚBLICA DE COLOMBIA
SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO

Oficio N° 11738 de 23 de julio de 2021

Ref. Expediente N° NC2019/0008341

Señor(a)
LLC MICROSOFT TECHNOLOGY LICENSING

TÍTULO DE LA SOLICITUD: ***“ANÁLISIS DE SEÑALES MÚLTIPLES PARA LA IDENTIFICACIÓN DE ÁMBITO AFECTADO”***

NÚMERO DE SOLICITUD INTERNACIONAL: PCT/US2018/017817

FECHA DE PRESENTACIÓN INTERNACIONAL: 12 de febrero de 2018.

PRIORIDAD(ES): US, 15/431,391, 13 de febrero de 2017.

Como resultado del examen de patentabilidad realizado a la solicitud indicada en la referencia, atendiendo a lo consagrado en el artículo 45 de la Decisión 486 de 2000, se le comunica que esta Dirección ha encontrado que la materia objeto de solicitud no cumple con algunos requisitos establecidos en la Decisión, con fundamento en los siguientes aspectos:

1. 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, 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 al momento de realizar el examen de patentabilidad consagrado en el artículo 45 de la Decisión 486. Por lo tanto, se estudiarán las reivindicaciones 1 a 15 del radicado N° NC2019/0008341 del 30 de julio de 2019.

El problema planteado en esta solicitud consiste en la necesidad de detectar amenazas para servicios en línea.

Para resolver este problema técnico, la solicitud en estudio proporciona sistemas, métodos y dispositivos de almacenamiento legible por computadora que modaliza instrucciones ejecutables de procesador para detectar máquinas huésped comprometidas. Se reciben señales de seguridad por un analizador de anormalidad de señal para determinar un nivel de anormalidad para una acción dada en el servicio en línea que se está asegurando. En un gran servicio en línea, se espera que grupos de dispositivos se comporten igual cuando funcionan correctamente y, por lo tanto, los comportamientos que no son comunes son tratados con mayor sospecha. Los resultados de detección clasificados son agregados de acuerdo con diversas poblaciones de dispositivos o sub-comportamientos y las puntuaciones de anormalidad se pasan a un analizador de señales múltiples, que recoge los resultados de detección a través de ventanas enrollables de tiempo y los divide en diversos ámbitos basados en el dispositivo para análisis para determinar si debe generarse una alerta de que un determinado dispositivo está comprometido (Descripción, Párr. 37).

2. De la solicitud de patente

2.1. Título

El nombre de la invención de que se trata en el artículo 27 literal d) de la Decisión 486 deberá reflejar el objeto y el campo industrial con el cual se relaciona la misma y ser



Oficio N° 11738 de 23 de julio de 2021

Ref. Expediente N° NC2019/0008341

concordante con la materia descrita y las reivindicaciones de la solicitud. El nombre no podrá referirse a nombres personales, marcas de productos o nombres de fantasía.

El solicitante en el escrito radicado bajo el N° NC2019/0008341 el 30 de julio de 2019, tituló la invención como: “ANÁLISIS DE SEÑALES MÚLTIPLES PARA LA IDENTIFICACIÓN DE ÁMBITO AFECTADO”. Este título no se relaciona con el objeto de la solicitud contenido en la descripción y las reivindicaciones, por lo cual se sugiere el título siguiente: “MÉTODO, SISTEMA Y DISPOSITIVO DE ALMACENAMIENTO DE ANÁLISIS DE SEÑALES MÚLTIPLES PARA LA IDENTIFICACIÓN DE ÁMBITO AFECTADO”.

2.2. Reivindicaciones (Art. 30 Decisión 486)

Se sugiere incluir entre paréntesis () los números de referencia de cada uno de los elementos que hacen parte de la invención de acuerdo con la numeración empleada en los dibujos, con el fin, de hacer más fácil la comprensión de la materia reivindicada.

3. Determinación del Estado de la Técnica

La fecha para determinar el estado de la técnica es el 13 de febrero de 2017 que corresponde a la fecha de presentación de la solicitud de prioridad.

Consultadas las fuentes de información con que se cuenta, se encontraron los siguientes documentos que anticipan el objeto de esta solicitud:

Ítem	Documento	Título	Fecha de Publicación
D1	US2007294187A1	“System and method for anomaly detection”	20 de diciembre de 2007
D2	US8122122B1	“Event monitoring and collection”	21 de febrero de 2012
D3	US9516053B1	“Network security threat detection by user/user-entity behavioral analysis”	6 de diciembre de 2016

El documento D1¹ divulga un sistema y método para detectar una o más anomalías en una pluralidad de observaciones. En una realización ilustrativa, las observaciones son observaciones de red en tiempo real recopiladas de un flujo de tráfico de red. El método incluye realizar una descomposición discreta de las observaciones e introducir variables derivadas para aumentar la eficiencia del almacenamiento y las consultas. A continuación, se genera un modelo matemático, como un modelo de independencia condicional, a partir de los datos formateados. Los datos formateados también se utilizan para construir tablas de frecuencia que mantienen un recuento preciso de la ocurrencia de variables específicas según lo indicado por el proceso de generación del modelo. Los datos formateados se aplican luego al modelo matemático para generar datos puntuados. A continuación, los datos puntuados se analizan para detectar anomalías (Resumen).

El documento D2² divulga sistemas, software y métodos para monitorear eventos en una computadora. En un conjunto de realizaciones, una aplicación de monitorización monitoriza eventos en una computadora monitorizada. Se puede analizar cada uno de los eventos monitoreados y, en base al análisis, se pueden recopilar algunos o todos los eventos monitoreados. Se pueden usar una variedad de reglas para analizar eventos. En algunos casos, los eventos recopilados se pueden poner en cola, por ejemplo, almacenando una representación de cada evento recopilado en una caché de eventos. Cuando la conectividad con un ordenador de supervisión está disponible, se puede establecer una conexión con el ordenador de supervisión y / o los eventos en cola pueden

¹<https://patentimages.storage.googleapis.com/95/6d/a3/3910e44492955c/US20070294187A1.pdf>
²<https://patentimages.storage.googleapis.com/8d/e5/df/d53e9e463d0ae5/US8122122.pdf>

Oficio N° 11738 de 23 de julio de 2021

Ref. Expediente N° NC2019/0008341

transmitirse al ordenador de supervisión. En un conjunto particular de realizaciones, la aplicación de monitorización está diseñada para evitar la detección por parte de un usuario del ordenador monitorizado (Resumen).

El documento D3³ divulga sistemas de procesamiento de datos distribuidos y, más particularmente, a la generación de inteligencia y al descubrimiento de actividades a partir de eventos en un sistema de procesamiento de datos distribuido (Col. 1, líneas 21 a 23).

4. Examen de Patentabilidad (Art. 14 Decisión 486)

4.1. Novedad (Art 16 Decisión 486)

La reivindicación 1 consiste en: “Un método para detectar ámbitos comprometidos en un servicio en línea (...)” (Radicado N° NC2019/0008341 del 30 de julio de 2019).

Tabla 1. Comparación de las características técnicas esenciales, con las del estado de la técnica

Características esenciales	D1
Un método para detectar ámbitos comprometidos en un servicio en línea, que comprende.	Un método para detectar una o más anomalías en una pluralidad de observaciones (...). (Resumen).
Recibir resultados de detección de comportamientos que ocurren en los dispositivos dentro del servicio en línea.	(...) las observaciones se reciben por unidad de tiempo (...). (Párr. 0104). (...) observaciones de red en tiempo real recopiladas de una pluralidad de tráfico de red (...). (Párr. 0030).
La puntuación de los resultados de detección basándose en cómo los comportamientos anómalos asociados están dentro del servicio en línea.	(...) con los resultados de la puntuación y la agrupación de los datos puntuados, el método (100) proporciona un procedimiento sencillo y robusto para detectar el comportamiento anómalo de la red (...). (Párr. 0081).
Organizar los resultados de detección puntuados de acuerdo con los ámbitos.	(...) categorizar tales variables en un número comparativamente pequeño de grupos. (Párr. 0051). (...) el análisis puede realizarse sobre los datos puntuados antes o después de un proceso de agrupamiento. (Párr. 0047).
Aplicar la lógica de detección de señales múltiples a un ámbito determinado para producir una puntuación de confianza que indica si el ámbito determinado está comprometido.	(...) lógica requerida en cada representación de datos. (Párr. 0073). (...) Una observación puede ser una cantidad multivariante que tiene una pluralidad de componentes donde cada componente tiene un valor que está asociado con cada variable de la observación (...). (Párr. 0030). Combinando un análisis comparativo de un modelo matemático, con los resultados de la puntuación y la agrupación de los datos puntuados, el método (100) proporciona un procedimiento simple y robusto para detectar el comportamiento anómalo de la red (...). (Párr. 0081).
Determinar si desea presentar una alerta de si el ámbito determinado está comprometido con base en la comparación de la puntuación de confianza con un umbral de alerta.	Si los datos puntuados están por encima del umbral, el método procede a procesar el bloque (362) (...) y se actualiza el gráfico visual en el bloque (358). A continuación, el método procede a realizar la agrupación del siguiente registro de datos puntuados. (Párr. 0110).

³<https://patentimages.storage.googleapis.com/76/44/f6/7ac79d3df5e4b3/US9516053.pdf>

Oficio N° 11738 de 23 de julio de 2021

Ref. Expediente N° NC2019/0008341

En respuesta a la determinación de que la alerta se va a presentar del ámbito determinado que está comprometido, generar y transmitir la alerta.	La figura 9 se muestra una captura de pantalla ilustrativa que muestra un gráfico visual generado con los resultados asociados con la realización de la puntuación y el agrupamiento descritos anteriormente (...). (Párr. 0112).
--	--

De acuerdo con la tabla anterior, las características esenciales del método de la reivindicación 1 habían sido divulgadas previamente en el documento D1, por lo tanto, la materia reivindicada no es nueva.

Asimismo, el documento D1 divulga las características de las reivindicaciones dependientes así:

- Reivindicación 2: (...) Los métodos pueden aplicarse a otros sistemas, como teléfonos fijos e inalámbricos, correo electrónico y correo del servicio postal, y análisis de infraestructura de transporte, redes eléctricas, transacciones con tarjetas de crédito y sistemas bancarios.
(Párr. 0024).

La reivindicación dependiente 2 tampoco cumple con el requisito de novedad.

La reivindicación 9 consiste en: “Un sistema que incluye un procesador y un dispositivo de almacenamiento de (...)” (Radicado N° NC2019/0008341 del 30 de julio de 2019).

Tabla 2. Comparación de las características técnicas esenciales, con las del estado de la técnica

Características esenciales	D1
Un sistema.	Un sistema para detectar una o más anomalías en una pluralidad de observaciones (...). (Resumen).
Que incluye un procesador y un dispositivo de almacenamiento de memoria que almacena instrucciones que cuando se ejecutan por el procesador ofrecen detectar ámbitos comprometidos en un servicio en línea, que comprende.	(...) La computadora de propósito general también puede incluir memoria de acceso aleatorio (RAM) (18), almacenamiento en disco duro (20), memoria de solo lectura (ROM) (22), un módem (26) y un coprocesador gráfico (28) (...). (Párr. 0028). Un sistema para detectar una o más anomalías en una pluralidad de observaciones (...). (Resumen).
Un calificador de anomalía de firma, configurado para.	(...) puntuación que puede detectarse como anómala (...). (Párr. 0085).
Recibir un determinado resultado de detección de un evento observado que ocurre en el servicio en línea.	(...) las observaciones se reciben por unidad de tiempo (...). (Párr. 0104). (...) observaciones de red en tiempo real recopiladas de una pluralidad de tráfico de red (...). (Párr. 0030).
Determinar el grado al cual un comportamiento asociado con el determinado resultado de detección ha sido anteriormente	Durante el proceso de puntuación (305), a cada registro de datos puntuados se le asigna un valor numérico real para indicar la sorpresa relativa dentro del contexto de todos los datos procesados por el modelo matemático en el bloque (118) (...) Una vez que se han clasificado los resultados de la puntuación, los datos (126) puntuados, generados por el proceso (305) (...) Los datos (126) puntuados se comparan luego con el umbral para determinar si se han detectado una o más anomalías.

Oficio N° 11738 de 23 de julio de 2021

Ref. Expediente N° NC2019/0008341

observado que ocurre en el servicio en línea; y.	(Párr. 0078). (...) cada rango contiene el rango correspondiente a la variable anterior (...). (Párr. 0061).
Producir una puntuación de anomalía que será asociada con el resultado de detección dado basándose en el grado al cual el comportamiento ha sido anteriormente observado; y.	(...) El procesador (12) está además programado para generar datos puntuados aplicando una colección de datos al primer modelo matemático, y luego para analizar los datos puntuados para detectar una o más anomalías. (Párr. 0032). Durante el proceso de puntuación (305), a cada registro de datos puntuados se le asigna un valor numérico real para indicar la sorpresa relativa dentro del contexto de todos los datos procesados por el modelo matemático en el bloque (118) (...) Una vez que se han clasificado los resultados de la puntuación, los datos (126) puntuados, generados por el proceso (305) (...) Los datos (126) puntuados se comparan luego con el umbral para determinar si se han detectado una o más anomalías. (Párr. 0078). (...) cada rango contiene el rango correspondiente a la variable anterior (...). (Párr. 0061).
Un detector de señales múltiples en comunicación con el calificador de anomalía de firma, configurado para.	(...) Una observación puede ser una cantidad multivariante que tiene una pluralidad de componentes donde cada componente tiene un valor que está asociado con cada variable de la observación (...). (Párr. 0030). Combinando un análisis comparativo de un modelo matemático, con los resultados de la puntuación y la agrupación de los datos puntuados, el método (100) proporciona un procedimiento simple y robusto para detectar el comportamiento anómalo de la red (...). (Párr. 0081).
Recibir uno o más resultados de detección que comparten un ámbito en el servicio en línea con el resultado de detección dado.	(...) las observaciones son observaciones de red en tiempo real recopiladas de una pluralidad de tráfico de red que pueden incluir, a modo de ejemplo no limitativo, direcciones de Protocolo de Internet (IP), números de puerto, hora, protocolo y tamaño de carga útil. Los expertos en la técnica apreciarán que una observación también puede denominarse registro de datos. (Párr. 0030). (...) Una vez que se han clasificado los resultados de la puntuación, los datos puntuados (126), generados por el proceso (305), se comunican al analista (...). (Párr. 0078).
Recibir, del calificador de anomalía de firma, la puntuación de anomalía asociada con el resultado de detección.	(...) puntuación que puede detectarse como anómala (...). (Párr. 0085). (...) En el bloque (350), el método proporciona la recepción de datos puntuados (...). (Párr. 0107).
Extraer las características de los resultados de detección del ámbito, las características incluyendo la puntuación de anomalía.	En una forma, la recopilación de datos utilizada para generar los datos puntuados es la misma que la de los datos extraídos de las observaciones. (Párr. 0006).
Generar una puntuación de confianza basándose en las características extraídas de si el ámbito está comprometido.	(...) El procesador (12) se programa además para generar datos puntuados aplicando una colección de datos al primer modelo matemático, y luego para analizar los datos puntuados para detectar una o más anomalías. (Párr. 0032). En la realización ilustrativa, el modelo matemático que el procesador (20) está programado para generar es un modelo de independencia condicional. Este modelo de independencia condicional se compone de

Oficio N° 11738 de 23 de julio de 2021

Ref. Expediente N° NC2019/0008341

	una relación matemática que representa las dependencias entre las variables del sistema. (Párr. 0033).
--	---

De acuerdo con la tabla anterior, las características esenciales del sistema de la reivindicación 9 habían sido divulgadas previamente en el documento D1, por lo tanto, la materia reivindicada no es nueva.

Asimismo, el documento D1 divulga las características de las reivindicaciones dependientes así:

- Reivindicación 10: Los datos direccionales son datos que se miden en una escala que se repite, como las horas del día o las direcciones angulares. Por ejemplo, se sabe que el tiempo entre las 11:00 a. m. Y la 1:00 p. m. Es de 2 horas, no las 10 horas que podría devolver una operación matemática estándar (...).
(Párr. 0052).
- Reivindicación 11: En la realización preferida, el desbordamiento puede evitarse durante un período de tiempo arbitrariamente largo alargando el tiempo de duplicación de los recuentos entrantes (...).
(Párr. 0104).
- Reivindicación 14: El sistema y los métodos ilustrativos de detección de anomalías se han desarrollado para ayudar a un analista de seguridad a identificar, revisar y evaluar el comportamiento anómalo del tráfico de la red (...).
(Párr. 0024).
(...) Una vez que se han clasificado los resultados de la puntuación, los datos puntuados (126), generados por el proceso (305), se comunican al analista. Durante el análisis (307), el analista inspecciona los datos puntuados con valores de sorpresa relativamente altos (...).
(Párr. 0078).

Las reivindicaciones dependientes 10, 11 y 14 tampoco cumplen con el requisito de novedad.

La reivindicación 15 consiste en: “*Un dispositivo de almacenamiento legible por computadora que incluye instrucciones (...)*” (Radicado N° NC2019/0008341 del 30 de julio de 2019).

Tabla 3. Comparación de las características técnicas esenciales, con las del estado de la técnica

Características esenciales	D1
Un dispositivo de almacenamiento legible por computadora que incluye instrucciones ejecutables por procesador para detectar ámbitos comprometidos en un servicio en línea, que comprende.	Un sistema y método para detectar una o más anomalías en una pluralidad de observaciones (...). (Resumen). (...) Estas instrucciones legibles por máquina pueden residir en varios tipos de soportes portadores de señales. A este respecto, un aspecto de la presente invención se refiere a un producto programado, que comprende medios portadores de señales que incorporan de manera tangible un programa de instrucciones legibles por máquina ejecutables por un procesador de datos digitales como la CPU (12) para la computadora de propósito general (10). (Párr. 0038).
Recibir resultados de detección de comportamientos que	(...) las observaciones se reciben por unidad de tiempo (...). (Párr. 0104).

Oficio N° 11738 de 23 de julio de 2021

Ref. Expediente N° NC2019/0008341

ocurren en los dispositivos dentro del servicio en línea.	(...) observaciones de red en tiempo real recopiladas de una pluralidad de tráfico de red (...). (Párr. 0030).
La puntuación de los resultados de detección basándose en cómo los comportamientos anómalos asociados están dentro del servicio en línea.	(...) se han clasificado los resultados de la puntuación, los datos puntuados (126), generados por el proceso (305), se comunican al analista. Durante el análisis (307), el analista inspecciona los datos puntuados con valores de sorpresa relativamente altos. En una realización ilustrativa, los datos puntuados se analizan identificando al menos un umbral. Los datos (126) puntuados se comparan luego con el umbral para determinar si se han detectado una o más anomalías. (Párr. 0078).
Organizar los resultados de detección calificados según los ámbitos, en donde un ámbito dado está asociado con un dispositivo dado o una determinada cuenta de usuario en el servicio en línea.	(...) categorizar tales variables en un número comparativamente pequeño de grupos. (Párr. 0051). (...) el análisis puede realizarse sobre los datos puntuados antes o después de un proceso de agrupamiento. (Párr. 0047). (...) Los métodos pueden aplicarse a otros sistemas, como teléfonos fijos e inalámbricos, correo electrónico y correo del servicio postal., y análisis de infraestructura de transporte, redes eléctricas, transacciones con tarjetas de crédito y sistemas bancarios. (Párr. 0024).
Aplicar la lógica de detección de señales múltiples al ámbito determinado para producir una puntuación de confianza que indica si el ámbito determinado está comprometido.	(...) lógica requerida en cada representación de datos. (Párr. 0073). (...) Una observación puede ser una cantidad multivariante que tiene una pluralidad de componentes donde cada componente tiene un valor que está asociado con cada variable de la observación (...). (Párr. 0030). Combinando un análisis comparativo de un modelo matemático, con los resultados de la puntuación y la agrupación de los datos puntuados, el método (100) proporciona un procedimiento simple y robusto para detectar el comportamiento anómalo de la red (...). (Párr. 0081).
Determinar si alertar a un analista del ámbito determinado que está comprometido en función de comparar la puntuación de confianza con un umbral de alerta; y.	Si los datos puntuados están por encima del umbral, el método procede a procesar el bloque (362) (...) y se actualiza el gráfico visual en el bloque (358). A continuación, el método procede a realizar la agrupación del siguiente registro de datos puntuados. (Párr. 0110).
En respuesta a la determinación de que el analista va a ser alertado del ámbito determinado que está comprometido, generar y transmitir una alerta.	La figura 9 se muestra una captura de pantalla ilustrativa que muestra un gráfico visual generado con los resultados asociados con la realización de la puntuación y el agrupamiento descritos anteriormente (...). (Párr. 0112).

De acuerdo con la tabla anterior, las características esenciales del dispositivo de almacenamiento legible por computadora de la reivindicación 15 habían sido divulgadas previamente en el documento D1, por lo tanto, la materia reivindicada no es nueva.

4.2. Nivel Inventivo (Art. 18 Decisión 486)

La reivindicación 6 consiste en: “El método de acuerdo con la reivindicación 1, en donde los resultados de detección (...)” (Radicado N° NC2019/0008341 del 30 de julio de 2019).

Tabla 4. Comparación de las características técnicas esenciales, con las del estado de la técnica:

Características esenciales	D1	D2
----------------------------	----	----

Oficio N° 11738 de 23 de julio de 2021

Ref. Expediente N° NC2019/0008341

El método de acuerdo con la reivindicación 1, en donde los resultados de detección desde.	Un método para detectar una o más anomalías en una pluralidad de observaciones (...). (Resumen).	(...) métodos para monitorear eventos en una computadora (...) (Resumen).
Una ventana de tiempo más pequeña, que comprende varios minutos de resultados de detección.	No menciona.	Configura el filtro de recopilación para recopilar eventos de prólogo dentro de una ventana de dos minutos antes del evento de interés. (Col. 16, líneas 12 a 14).
Y una ventana de tiempo más grande, que comprende varios días de resultados, se incluyen en los ámbitos.	(...) Las observaciones pueden ser una colección de observaciones recopiladas en el transcurso de una hora, un día, varias semanas o varios meses. (Párr. 0026).	No menciona.

El documento D1 se considera el estado de la técnica más cercano a la invención definida en la reivindicación 6 porque divulga un método para detectar una o más anomalías en una pluralidad de observaciones. En una realización ilustrativa, los datos se extraen de las observaciones y se formatean para facilitar el procesamiento posterior (...) (Párr. 0005).

La diferencia entre la invención definida en la reivindicación 6 y método divulgado de D1 consiste en una ventana de tiempo más pequeña, que comprende varios minutos de resultados de detección.

No se evidencia un efecto asociado al incluir una ventana de tiempo más pequeña, que comprende varios minutos de resultados de detección en el método para detectar ámbitos comprometidos en un servicio de línea.

Por lo tanto, el problema técnico objetivo que pretende resolver esta invención se puede formular así: ¿Cómo modificar el método conocido en D1 con el fin de obtener un método alternativo?

Sin embargo, el incluir una ventana de tiempo más pequeña, que comprende varios minutos de resultados de detección para obtener el método alternativo para detectar ámbitos comprometidos en un servicio en línea, ya está divulgado en el documento D2 que se refiere a configura el filtro de recopilación para recopilar eventos de prólogo dentro de una ventana de dos minutos antes del evento de interés (Col. 16, líneas 12 a 14).

En consecuencia, la persona normalmente versada en la materia estaría motivada a incluir una ventana de tiempo más pequeña, que comprende varios minutos de resultados de detección del documento D2 en el método de D1, para así llegar al objeto de la reivindicación 6. Por lo cual se considera obvia.

La reivindicación 7 consiste en: “El método de acuerdo con la reivindicación 1, en donde la aplicación de lógica de (...)” (Radicado N° NC2019/0008341 del 30 de julio de 2019).

Tabla 5. Comparación de las características técnicas esenciales, con las del estado de la técnica:

Características esenciales	D1	D3
----------------------------	----	----

Oficio N° 11738 de 23 de julio de 2021

Ref. Expediente N° NC2019/0008341

El método de acuerdo con la reivindicación 1.	Un método para detectar una o más anomalías en una pluralidad de observaciones (...). (Resumen).	Una variedad de técnicas y mecanismos para detectar anomalías y amenazas relacionadas con la seguridad en un entorno de red informática (...). (Resumen).
En donde la aplicación de lógica de detección de señales múltiples al ámbito determinado para producir la puntuación de confianza además comprende	(...) lógica requerida en cada representación de datos. (Párr. 0073). (...) Una observación puede ser una cantidad multivariante que tiene una pluralidad de componentes donde cada componente tiene un valor que está asociado con cada variable de la observación (...). (Párr. 0030).	No menciona.
Seleccionar un modelo predictivo.	No menciona.	Una pluralidad de modelos (incluidos los modelos de aprendizaje automático) para lograr un mejor rendimiento predictivo en la puntuación de anomalías y reducir los falsos positivos. (Col. 106, líneas 1 a 3).
Extraer características de los resultados de detección.	En una forma, la recopilación de datos utilizada para generar los datos puntuados es la misma que la de los datos extraídos de las observaciones. (Párr. 0006).	No menciona.
La puntuación de las características para la conversión en características valoradas numéricamente; y.	La transformación descrita por esta descomposición mapea cada punto en el intervalo continuo a un vector binario que representa el intervalo, o bin, que contiene la variable. (Párr. 0054). Durante el proceso de puntuación (305), a cada registro de datos puntuados se le asigna un valor numérico real para indicar la sorpresa relativa dentro del contexto de todos los datos procesados por el modelo matemático en el bloque (118) (...) Una vez que se han clasificado los resultados de la puntuación, los datos (126) puntuados, generados por el proceso (305) (...) Los datos (126) puntuados se comparan luego con el umbral para determinar si se han detectado una o más anomalías. (Párr. 0078).	No menciona.
Proporcionar las características.	(...) El modelo matemático es capaz de adaptarse dinámicamente a los cambios en las características de los datos, como los recuentos relativos de ocurrencias de variables. En el método ilustrativo de generación automatizada de modelos, el modelo matemático es un modelo de independencia condición. (Párr. 0082)	En algunas realizaciones, generar la pluralidad de puntuaciones de características incluye analizar el tiempo de las comunicaciones asociadas con la entidad (interna o externa) durante un período de tiempo y asignar una puntuación de característica. (Col. 104, líneas 30 a 33).

Oficio N° 11738 de 23 de julio de 2021

Ref. Expediente N° NC2019/0008341

Del modelo predictivo.	No menciona.	Una pluralidad de modelos (incluidos los modelos de aprendizaje automático) para lograr un mejor rendimiento predictivo en la puntuación de anomalías y reducir los falsos positivos. (Col. 106, líneas 1 a 3).
Para generar la puntuación de confianza.	Combinando un análisis comparativo de un modelo matemático, con los resultados de la puntuación y la agrupación de los datos puntuados, el método (100) proporciona un procedimiento simple y robusto para detectar el comportamiento anómalo de la red (...). (Párr. 0081).	En el que la puntuación de características es indicativa de un nivel de confianza en que las comunicaciones son generadas por una máquina. (Col. 104, líneas 33 a 35).

El documento D1 se considera el estado de la técnica más cercano a la invención definida en la reivindicación 7 porque divulga un método para detectar una o más anomalías en una pluralidad de observaciones. En una realización ilustrativa, los datos se extraen de las observaciones y se formatean para facilitar el procesamiento posterior (...) (Párr. 0005).

La diferencia entre la invención definida en la reivindicación 7 y método divulgado de D1 consiste en seleccionar un modelo predictivo.

El efecto que se logra al incluir seleccionar un modelo predictivo es proporcionar una puntuación de confianza de si el ámbito del que se extrajo el vector de característica está exhibiendo comportamientos maliciosos.

Por lo tanto, el problema técnico objetivo que pretende resolver esta invención se puede formular así: ¿Cómo modificar el método conocido en D1 con el fin de proporcionar una puntuación de confianza de si el ámbito del que se extrajo el vector de característica está exhibiendo comportamientos maliciosos?

Sin embargo, el incluir seleccionar un modelo predictivo para proporcionar una puntuación de confianza de si el ámbito del que se extrajo el vector de característica está exhibiendo comportamientos maliciosos, ya está divulgado en el documento D3 que se refiere a una pluralidad de modelos (incluidos los modelos de aprendizaje automático) para lograr un mejor rendimiento predictivo en la puntuación de anomalías y reducir los falsos positivos (Col. 106, líneas 1 a 3).

En consecuencia, la persona normalmente versada en la materia estaría motivada a incluir seleccionar un modelo predictivo del documento D3 en el método de D1, para así llegar al objeto de la reivindicación 7. Por lo cual se considera obvia.

La reivindicación 8 consiste en: “El método de acuerdo con la reivindicación 7, en donde el modelo predictivo (...)” (Radicado N° NC2019/0008341 del 30 de julio de 2019).

El documento D1 se considera el estado de la técnica más cercano a la invención definida en la reivindicación 8 porque divulga un método para detectar una o más anomalías en una pluralidad de observaciones. En una realización ilustrativa, los datos se extraen de las observaciones y se formatean para facilitar el procesamiento posterior (...) (Párr. 0005).

Oficio N° 11738 de 23 de julio de 2021

Ref. Expediente N° NC2019/0008341

La diferencia entre la invención definida en la reivindicación 8 y método divulgado de D1 consiste en que el modelo predictivo se genera y selecciona en función de un proceso de aprendizaje continuo de máquina.

El efecto que se logra al incluir que el modelo predictivo se genere y seleccione en función de un proceso de aprendizaje continuo de máquina es determinar si un determinado dispositivo (o usuario o proceso) se está comportando maliciosamente con base en los resultados de detección puntuados presentados en el ámbito.

Por lo tanto, el problema técnico objetivo que pretende resolver esta invención se puede formular así: ¿Cómo modificar el método conocido en D1 con el fin de determinar si un determinado dispositivo (o usuario o proceso) se está comportando maliciosamente con base en los resultados de detección puntuados presentados en el ámbito?

Sin embargo, que el modelo predictivo se genere y seleccione en función de un proceso de aprendizaje continuo de máquina para determinar si un determinado dispositivo (o usuario o proceso) se está comportando maliciosamente con base en los resultados de detección puntuados presentados en el ámbito, ya está divulgado en el documento D3 que se refiere a técnicas de aprendizaje por conjuntos para procesar la pluralidad de puntuaciones de características de acuerdo con una pluralidad de modelos (incluidos los modelos de aprendizaje automático) para lograr un mejor rendimiento predictivo en la puntuación de anomalías y reducir los falsos positivos (Col. 105, líneas 66 a 67 y Col. 106, líneas 1 a 3).

En consecuencia, la persona normalmente versada en la materia estaría motivada a incluir que el modelo predictivo se genere y seleccione en función de un proceso de aprendizaje continuo de máquina del documento D3 en el método de D1, para así llegar al objeto de la reivindicación 8. Por lo cual se considera obvia.

5. Conclusión con respecto a novedad y/o nivel inventivo

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

Ítem	Documento	Reivindicaciones afectadas	Requisito que afecta
D1	US2007294187A1	1, 2, 9, 10, 11, 14 y 15	Novedad
		6 a 8	Nivel Inventivo
D2	US8122122B1	6	Nivel Inventivo
D3	US9516053B1	7 y 8	Nivel Inventivo

En cumplimiento del artículo 45 de la Decisión 486 de 2000, 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 modifica el capítulo reivindicatorio, deberá observar las instrucciones contenidas en el numeral 1.2.2.1.1., del Capítulo Primero del Título X de la Circular Única de esta Superintendencia. De igual forma, deberá tener presente que de conformidad con el literal a) del numeral 1.2.2.5.1. de la norma ibidem, será necesario acreditar el pago de la tasa por concepto de modificación a solicitudes en trámites, de conformidad con el valor establecido en la resolución de tasas vigentes.

Oficio N° 11738 de 23 de julio de 2021

Ref. Expediente N° NC2019/0008341

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 recurso alguno en actuación administrativa.



Edna Marcela Ramirez Orozco
DIRECTORA DE NUEVAS CREACIONES



Oficio N° 11738 de 23 de julio de 2021

Ref. Expediente N° NC2019/0008341

INFORME DE BÚSQUEDA
EXAMEN DE PATENTABILIDAD

Solicitud No.		Examen de patentabilidad							
NC2019/0008341		1°	X	2°		3°		Revoca	
Solicitud Internacional No.		Fecha solicitud internacional: (DD/MM/AÑO)							
PCT/US2018/017817		12 de febrero de 2018							
Fecha de determinación estado de la técnica (DD/MM/AÑO)				Prioridad		Presentación			
13/02/2017				X					
Solicitante									
LLC MICROSOFT TECHNOLOGY LICENSING									
Reivindicaciones que no son objeto de búsqueda por:									
Art. 14	-	Art. 15	-	Art. 20	-	Art. 25 (Falta de unidad de invención)		-	

CRITERIOS DE BÚSQUEDA	
Reivindicaciones objeto de búsqueda	1 a 15
Palabras clave utilizadas	Multi-signal, analysis, compromis*, scope, identi*, method, detect*, online, service, receiv*, behavior*, logic, confidence, score, alert, confidence, threshold.
Clasificaciones utilizadas para la búsqueda	CIP: G06F 21/55, H04L 29/06

DOCUMENTOS CONSIDERADOS RELEVANTES (Documentos patente, Literatura no patente (LNP): Artículos, catálogos, etc.)					
Informes de búsqueda / Bases de datos consultadas	N° de solicitud de patente / N° de patente / Autor LNP(1)	Fecha de Publicación /Presentación (DD/MM/AAAA)	Reivindicaciones /Secuencias afectadas	Citas relevantes del estado de la técnica	Categoría del documento citado(2)
SIPI	NC2018/0008614	16/08/2018	-	-	E
WIPO	US2007294187A1	20/12/2007	1, 2, 9, 10, 11, 14 y 15	1 Resumen; Párr. 0104; Párr. 0030; Párr. 0051; Párr. 0047; Párr. 0073; Párr. 0030; Párr. 0081; Párr. 0110; Párr. 0112;.	X
				2 Párr. 0024.	
				9 Resumen; Párr. 0028; Párr. 0085; Párr. 0030; Párr. 0104; Párr. 0032; Párr. 0078; Párr. 0061; Párr. 0081; Párr. 0107; Párr. 0006; Párr. 0033.	
				10 Párr. 0052.	
				11 Párr. 0104.	
				14 Párr. 0024; Párr. 0078.	
				15 Resumen; Párr. 0038; Párr. 0030; Párr. 0078; Párr. 0051; Párr. 0047; Párr. 0024; Párr. 0073; Párr. 0030; Párr. 0081; Párr. 0011; Párr. 0112.	Y

Oficio N° 11738 de 23 de julio de 2021

Ref. Expediente N° NC2019/0008341

	US8122122B1	21/02/2012	6	6 Resumen; Párr. 0026. 7 Resumen; Párr. 0030; Párr. 0006; Párr. 0054; Párr. 0078; Párr. 0082; Párr. 0081. 8 Párr. 0005.	Y
	EP2908495A1	19/08/2015	-	6 Resumen; Col. 16, líneas 12 a 14.	A
				-	
USPTO	US2018004948A1	4/01/2018	-	-	E
	US9338187B1	10/05/2016	-	-	A
	US2015235152A1	20/08/2015	-	-	A
	US2017093902A1	27/11/2008	-	-	A
	US8793151B2	29/07/2014	-	-	A
	US9690933B1	27/06/2017	-	-	E
	US2008295172A1	27/11/2008	-	-	A
	US2007294768A1	20/12/2007	-	-	A
	US7784099B2	24/08/2010	-	-	A
	US2008189788A1	7/08/2008	-	-	A
	US9654485B1	16/05/2017	-	-	E
	US8448247B2	21/05/2013	-	-	A
	US9117076B2	25/08/2015	-	-	A
Patbase	US2016308725	20/10/2016	-	-	A
Epoquenet	US2010202299	12/08/2010	-	-	A
Googlepatent	US9516053B1	6/12/2016	7 y 8	7 Resumen; Col. 106, líneas 1 a 3; Col. 104, líneas 30 a 33; Col. 104; líneas 33 a 35. 8 Col. 105, líneas 66 a 67 y Col. 106, líneas 1 a 3.	Y
(1) Cita completa literatura no patente (LNP)					
Apellido, A. A. (Fecha). Título del artículo. Nombre de la revista. Volumen(Número), pp-pp.					
O					
Apellido, A. A. (Fecha). Título del artículo. Nombre de la revista. Recuperado de http://xxxxxxx.					
(2) Categorías de documentos citados					
“A” Documento que define el estado general de la técnica no considerado como particularmente relevante. “E” Solicitud de patente o patente anterior pero publicada en la fecha de presentación internacional o en fecha posterior. “L” Documento citado para llamar la atención sobre por ejemplo, dudas acerca de una reivindicación de prioridad o para determinar la fecha de publicación de otra cita, siempre van acompañados de una explicación, por la cual se citan. “O” Documento del tipo actas de conferencia, este tipo de documentos siempre estará acompañado por otra letra que indique la pertinencia del documento, por ejemplo, O,X, O,Y o bien O,A. “P” Documento publicado antes de la fecha de presentación internacional pero con posterioridad a la fecha de prioridad reivindicada. “T” Documento publicado en fecha posterior a la de presentación o la de prioridad de la solicitud internacional y no entra en conflicto con dicha solicitud, pero puede ser útil para la mejor comprensión del principio o teoría en que se basa la invención, o para demostrar que el razonamiento o los hechos en los que se basa dicha invención son incorrectos. “X” Documento particularmente relevante; la invención reivindicada no puede considerarse nueva o que implique una actividad inventiva por referencia al documento aisladamente considerado. “Y” Documento particularmente relevante; la invención reivindicada no puede considerarse que implique una actividad inventiva cuando el documento se asocia a otro u otros documentos de la misma naturaleza, cuya combinación resulta evidente para un experto en la materia.					
Fecha del reporte de búsqueda: 24/06/2021					
Examinador: FREDDY ALEXANDER VELANDIA VIVAS					

Oficio N° 11738 de 23 de julio de 2021

Ref. Expediente N° NC2019/0008341

