

REPÚBLICA DE COLOMBIA
SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO

Oficio N° 7020 de 7 de mayo de 2021

Ref. Expediente N° NC2019/0004599

Señor(a)
LLC MICROSOFT TECHNOLOGY LICENSING

TÍTULO DE LA SOLICITUD: “APARATO Y MÉTODOS PARA SERVICIO DE SEGURIDAD DEL INTERNET DE LAS COSAS”

NÚMERO DE SOLICITUD INTERNACIONAL: PCT/US2017/058926

FECHA DE PRESENTACIÓN INTERNACIONAL: 30 de octubre de 2017.

PRIORIDAD(ES): US, 15/344,461, 4 de noviembre de 2016.

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. Modificaciones presentadas (Art. 34 Decisión 486)

Se aceptan las modificaciones radicadas el 19 de abril de 2021, bajo el número NC2019/0004599, por ajustarse a los requisitos legales.

2. 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 20 del radicado N° NC2019/0004599 del 19 de abril de 2021.

El problema planteado en esta solicitud consiste en la necesidad de monitorizar, detectar y disminuir las amenazas de seguridad para los dispositivos de IoT utilizando la telemetría sobre el estado de seguridad del dispositivo de IoT y utilizando otros datos del entorno a partir de otros dispositivos de IoT.

Para resolver este problema técnico, la solicitud en estudio proporciona un aparato y métodos para garantizar la seguridad para los dispositivos de IoT permitiendo la detección de amenazas de seguridad tales como intrusiones y manipulación.

3. De la solicitud de patente

3.1. 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.

4. Determinación del Estado de la Técnica



Oficio N° 7020 de 7 de mayo de 2021

Ref. Expediente N° NC2019/0004599

La fecha para determinar el estado de la técnica es el 4 de noviembre de 2016 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	WO2016140912	“Behavioral analysis to automate direct and indirect local monitoring of internet of things device health”	9 de septiembre de 2016

El documento D1¹ divulga un método y aparato de análisis de comportamiento para automatizar el monitoreo del estado del dispositivo de Internet de las cosas (IoT) de manera directa y/o indirecta. En particular, el comportamiento normal asociado con un dispositivo IoT en una red IoT local puede modelarse de tal manera que los comportamientos observados en el dispositivo IoT puedan compararse con el comportamiento normal modelado para determinar si los comportamientos observados en el dispositivo IoT son normales o anómalos. En consecuencia, en un entorno IoT distribuido, los dispositivos "analizadores" más potentes pueden recopilar comportamientos localmente observados en otros dispositivos "observadores" (por ejemplo, más simples) y realizar análisis de comportamiento a través del entorno IoT distribuido para detectar anomalías que posiblemente indiquen ataques maliciosos, mal funcionamiento o otros asuntos que requieren servicio al cliente y/o atención adicional. Además, los dispositivos con capacidades suficientes pueden realizar análisis de comportamiento (local) en el dispositivo para detectar condiciones anómalas sin enviar comportamientos observados localmente a otro dispositivo agregador y/o dispositivo analizador (Resumen)

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

5.1. Novedad (Art 16 Decisión 486)

La reivindicación 1 consiste en: “Un aparato para la seguridad del internet de las cosas (IoT, por sus siglas en inglés), que comprende: (...)” (Radicado N° NC2019/0004599 del 19 de abril de 2021).

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

Características esenciales	D1
Un concentrador de IoT que incluye uno o más dispositivos.	(...) En un entorno IoT distribuido, los dispositivos "analizadores" más potentes pueden recopilar comportamientos observados localmente en otros dispositivos "observadores" (por ejemplo, más simples) (...) (Resumen).
Los dispositivos incluyen al menos una memoria adaptada para almacenar los datos en tiempo de ejecución para los dispositivos.	(...) Un módulo de software puede residir en RAM, memoria flash, ROM, EPROM, EEPROM, registros, disco duro, un disco extraíble, un CD-ROM o cualquier otra forma de medio de almacenamiento conocido en la técnica (...) (Párr. 00143).
Al menos un procesador que está adaptado para ejecutar el código ejecutable por procesador que, en respuesta a la ejecución, permite que el concentrador de IoT realice	(...) Un medio de almacenamiento ejemplar está acoplado al procesador de modo que el procesador pueda leer información y escribir información en el medio de almacenamiento (...) (Párr. 00143).

¹<https://patents.google.com/patent/WO2016140912A1/en?qoq=WO2016140912>

Oficio N° 7020 de 7 de mayo de 2021

Ref. Expediente N° NC2019/0004599

las acciones, que incluyen:	
Generar un modelo configurable de dispositivo de IoT.	(...) En el que el modelo que representa el comportamiento normal asociado con el dispositivo IoT (900) puede construirse a lo largo del tiempo en base a (...) los vectores de comportamiento (932) generados en la plataforma de monitoreo de salud en el dispositivo (910), vectores de comportamiento y / o modelos correspondientes a otros dispositivos en la red local de IoT (...) (Párr. 00102).
Almacenar un conjunto de reglas de seguridad que están asociadas con una condición esperada de al menos un dispositivo de IoT.	(...) Los umbrales u otros parámetros utilizados para detectar las anomalías pueden depender del contexto, ya que los umbrales de detección de anomalías u otros parámetros de detección de anomalías podrían reflejar condiciones normales o anormales en diferentes escenarios (...) (Párr. 00122).
El conjunto de reglas de seguridad estando basado en información de operación recibida de cada uno de una pluralidad de dispositivos de IoT.	(...) En el que el modelo que representa el comportamiento normal asociado con el dispositivo IoT (900) puede construirse a lo largo del tiempo en base a (...) los vectores de comportamiento (932) generados en la plataforma de monitoreo de salud en el dispositivo (910), vectores de comportamiento y / o modelos correspondientes a otros dispositivos en la red local de IoT (...) (Párr. 00102). (...) En el vector de comportamiento ejemplar (932) que se muestra arriba, las características de consumo de energía, temperatura interna y uso de la CPU tienen valores precisos, mientras que la conectividad a Internet comprende un valor binario, por lo que las características de consumo de energía, temperatura interna y uso de la CPU tienen una granularidad más fina que la función de conectividad a Internet (...) (Párr. 00101).
Recibir datos de IoT asociados con al menos un dispositivo de IoT cuando dicho al menos un dispositivo de IoT determina enviar los datos de IoT en respuesta a que se ha excedido un umbral basado en uno o más de los tipos de datos, en donde los datos de IoT son datos agregados que incluyen al menos dos tipos diferentes de datos.	En el caso de uso del dispositivo de IoT de refrigerador mostrado en la FIG. 16, el bloque (1620) puede incluir comparar el comportamiento observado en el dispositivo de IoT del refrigerador con uno o más modelos que indican un consumo de energía normal (o anormal), temperatura ambiente y valores de carga asociados con el dispositivo de IoT del refrigerador. (...) Como alternativa, en respuesta a la determinación en el bloque (1630) de que el valor asociado con la característica de comportamiento de consumo de energía excede el valor umbral, se pueden verificar una o más características de comportamiento adicionales para determinar si el consumo de energía indica una anomalía potencial que puede requerir servicio al cliente o una condición normal bajo las circunstancias (...) (Párr. 00129). En respuesta a los bloques (1630), (1640), (1650) que dan como resultado determinaciones respectivas de que el consumo de energía observado excede el valor umbral, la temperatura ambiente observada es normal o por debajo de lo normal, y la carga observada es normal o por debajo de lo normal, una condición anómala puede ser detectado e informado en el bloque (1670), que puede comprender la transmisión de los parámetros de comportamiento observados al servicio al cliente (...) y posiblemente también los valores de umbral en comparación con los parámetros de comportamiento observados (...) (Párr. 00130). En la arquitectura distribuida (1100) mostrada en la FIG. 11, el dispositivo de monitoreo siempre encendido (1110) puede recibir uno o más registros de acción (1122) de los dispositivos de observación (1112), (1114), los dispositivos de agregación (1116), (1118) y el monitor de tráfico de red (1120), en donde el dispositivo de monitoreo siempre encendido (1110) puede comprender un módulo de extracción de vectores de comportamiento (1130) configurado para mapear las características contenidas en los registros de acción (1122) en un espacio n-dimensional para extraer uno o más vectores de comportamiento (1132) que representan los comportamientos observados (...) (Párr. 00112). (...) En el vector de comportamiento ejemplar (932) que se muestra arriba, las características de consumo de energía, temperatura interna y uso de la CPU tienen valores precisos, mientras que la conectividad a Internet comprende un valor binario, por lo que las características de consumo de energía, temperatura interna y uso de la CPU tienen una granularidad más fina que la función de conectividad a Internet (...)

Oficio N° 7020 de 7 de mayo de 2021

Ref. Expediente N° NC2019/0004599

	(Párr. 00101).
Determinar, para cada dispositivo de IoT del al menos un dispositivo IoT, con base en los datos de IoT y en el modelo de dispositivo de IoT, si se infringió el conjunto de reglas de seguridad para el dispositivo IoT con base en información de operación recibida de cada uno de una pluralidad de dispositivos de IoT de tal manera que la determinación está basada en una combinación de al menos dos tipos diferentes de datos de al menos dos de la pluralidad de dispositivos de IoT considerados en conjunto.	(...) En varias realizaciones, los nodos analizadores (1070)-(1072) pueden analizar los vectores de comportamiento agregados de acuerdo con comparaciones con modelos específicos de marcas, versiones, etc., asociados con los dispositivos que corresponden a los comportamientos observados, que pueden obtenerse de los fabricantes o otros repositorios adecuados, basados en vectores de comportamiento de todos los dispositivos en la red IoT (1000) y un modelo específico para la red IoT (1000) y / o entradas e interacciones de usuarios asociados con la red IoT (1000), etc. En consecuencia, en lugar de detectar las anomalías de comportamiento basándose en una sola característica, los nodos analizadores (1070)-(1072) pueden usar el aprendizaje automático para detectar las anomalías de comportamiento mediante la evaluación de los vectores de comportamiento en combinación con modelos que se construyen a lo largo del tiempo para indicar un comportamiento normal, en general estados ambientales, etc. (Párr. 00109).
Enviar selectivamente una alerta con base en la determinación.	En diversas realizaciones, el módulo de análisis (1140) puede invocar uno o más actuadores (1170) para remediar una o más anomalías de comportamiento detectadas en los vectores de comportamiento analizados (1132) (...) (Párr. 00113).

De acuerdo con la tabla anterior, las características esenciales del aparato 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: (...) En diversas realizaciones, los umbrales de detección de anomalías o los parámetros de detección de anomalías se pueden aprender a lo largo del tiempo y personalizarse según los requisitos específicos del usuario o los patrones de uso según el dispositivo, lo que puede garantizar que no se utilice un solo modelo para detectar todas las anomalías y, por lo tanto potencialmente aumentar las tasas de falsos positivos y / o las tasas de falsos negativos (...) (Párr. 00122).
- Reivindicaciones 3 y 4: En la red IoT distribuida (1000) mostrada en la FIG. 10, los dispositivos configurados para operar en la función de observador comprenden altavoces exteriores (1012), (1014), altavoces interiores (1016), (1018), un termostato (1020), una lavadora (1022), un reloj (1024), una cafetera (1026), un altavoz de piso de la sala de estar (1028), un sistema de audio de estantería (1030), altavoces de cine en casa (1032), (1034) y un pomo de la puerta (1036), denominados colectivamente en el presente documento como nodos de observación (1012)-(1036). Además, los dispositivos configurados para operar en la función de agregador comprenden un refrigerador (1050) y un televisor (1052), denominados colectivamente en este documento como nodos de agregación (1050)-(1052), y los dispositivos configurados para operar en la función de analizador comprenden un teléfono inteligente (1070) y un enrutador inalámbrico o puerta de enlace doméstica (1072), denominada colectivamente en este documento como nodos analizadores (1070)-(1072) (...) (Párr. 00107). En la arquitectura distribuida (1100) mostrada en la FIG. 11, el dispositivo de monitoreo siempre encendido (1110) puede recibir uno o más registros de acción (1122) de los dispositivos de observación (1112), (1114), los dispositivos de agregación (1116), (1118) y el monitor de tráfico de red (1120) (...) (Párr. 00112).

Oficio N° 7020 de 7 de mayo de 2021

Ref. Expediente N° NC2019/0004599

- Reivindicación 5: (...) En cualquier caso, en el bloque (1620), el comportamiento observado en el dispositivo IoT del refrigerador se puede comparar con uno o más modelos que representan un comportamiento normal asociado con el dispositivo IoT del refrigerador y definir uno o más valores umbral normales y/o anormales que pueden utilizarse para detectar comportamientos anómalos. Por ejemplo, en diversas realizaciones, el uno o más modelos pueden incluir información que indica un consumo de energía normal (o anormal), temperatura ambiente, carga y/u otro estado adecuado asociado con el dispositivo IoT del refrigerador. En consecuencia, debido a que los valores de umbral que se monitorean para detectar las anomalías pueden ser normales o anormales dependiendo del contexto, las comparaciones realizadas en el bloque (1620) pueden usar más información específica de la ubicación (por ejemplo, clima local) para determinar los valores de umbral en comparación con el comportamiento observado en el dispositivo IoT del refrigerador en la medida en que dicha información contextual esté disponible (Párr. 00128).
- Reivindicación 6: Un dispositivo IoT puede tener un conjunto particular de atributos (por ejemplo, un estado o estado del dispositivo, como si el dispositivo IoT está encendido o apagado, abierto o cerrado, inactivo o activo, disponible para la ejecución de tareas u ocupado, etc., función de enfriamiento o calefacción, una función de monitoreo o grabación ambiental, una función de emisión de luz, una función de emisión de sonido, etc.) que puede ser integrada y / o controlada / monitoreada por una unidad central de procesamiento (CPU), microprocesador, ASIC, o similares, y configurados para conectarse a una red IoT, como una red ad-hoc local o Internet (...) (Párr. 0037).
- Reivindicación 7: En la red IoT distribuida (1000) mostrada en la FIG. 10, los dispositivos configurados para operar en la función de observador comprenden altavoces exteriores (1012), (1014), altavoces interiores (1016), (1018), un termostato (1020), una lavadora (1022), un reloj (1024), una cafetera (1026), un altavoz de piso de la sala de estar (1028), un sistema de audio de estantería (1030), altavoces de cine en casa (1032), (1034) y un pomo de la puerta (1036), denominados colectivamente en el presente documento como nodos de observación (1012)-(1036). Además, los dispositivos configurados para operar en la función de agregador comprenden un refrigerador (1050) y un televisor (1052), denominados colectivamente en este documento como nodos de agregación (1050)-(1052), y los dispositivos configurados para operar en la función de analizador comprenden un teléfono inteligente (1070) y un enrutador inalámbrico o puerta de enlace doméstica (1072), denominada colectivamente en este documento como nodos analizadores (1070)-(1072) (...) (Párr. 00107).
- Reivindicaciones 8 y 9: (...) En el vector de comportamiento ejemplar (932) que se muestra arriba, las características de consumo de energía, temperatura interna y uso de la CPU tienen valores precisos, mientras que la conectividad a Internet comprende un valor binario, por lo que las características de consumo de energía, temperatura interna y uso de la CPU tienen una granularidad más fina que la función de conectividad a Internet (...) (Párr. 00101). (...) El dispositivo IoT (900) puede monitorear un entorno local asociado con el mismo (por ejemplo, un acelerómetro que puede medir la aceleración y la inclinación, un sensor de temperatura que puede medir la temperatura interna y / o ambiental, un fotosensor que puede detectar la luz, una antena que puede monitorear las señales inalámbricas locales, instrumentos que pueden detectar la actividad del procesador, la actividad de la red, etc.) (...) (Párr. 0099).



Oficio N° 7020 de 7 de mayo de 2021

Ref. Expediente N° NC2019/0004599

- Reivindicación 10: (...) Los comportamientos de uso de un dispositivo IoT que es un termostato puede incluir a qué temperaturas está configurado el termostato en momentos específicos. En otro ejemplo, los comportamientos de uso de un dispositivo IoT que es un televisor inteligente puede incluir qué medios se ven en momentos específicos a través del televisor inteligente y con qué servidores interactúa el televisor inteligente en momentos específicos (...) (Párr. 0046).
- Reivindicación 11: (...) La simplicidad del dispositivo implica comportamientos relativamente limitados en los que pueden participar ciertos dispositivos de IoT, lo que puede brindar oportunidades con respecto al problema de servicio al cliente y el problema de seguridad porque ambos involucran anomalías de comportamiento al menos hasta cierto punto (por ejemplo, picos repentinos en el tráfico de red pueden indicar que un ataque de denegación de servicio (DoS) contra una computadora, la energía consumida durante un período de tiempo prolongado pueden indicar un dispositivo defectuoso, etc.) (Párr. 0005).
- Reivindicación 12: En diversas realizaciones, el módulo de análisis (1140) puede invocar uno o más actuadores (1170) para remediar una o más anomalías de comportamiento detectadas en los vectores de comportamiento analizados (1132) (...) (Párr. 00113).

Las reivindicaciones dependientes 2 a 12 tampoco cumplen con el requisito de novedad.

La reivindicación 13 consiste en: *“Un método para la seguridad del internet de las cosas (IoT, por sus siglas en inglés), que comprende: (...)”* (Radicado N° NC2019/0004599 del 19 de abril de 2021).

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

Características esenciales	D1
Generar un modelo configurable de dispositivo de IoT con base en información de operación recibida de cada uno de una pluralidad de dispositivos de IoT.	(...) Tener la información de ubicación, la información meteorológica y otra información relevante del contexto y/o el entorno local de los dispositivos informativos IoT (1416), (1418), (1420) puede ser útil para determinar los umbrales u otros parámetros utilizados para detectar las anomalías. Además, en diversas realizaciones, los umbrales de detección de anomalías o los parámetros de detección de anomalías se pueden aprender con el tiempo y personalizar según los requisitos específicos del usuario o los patrones de uso según el dispositivo específico (...) (Párr. 00122). (...) En el que el modelo que representa el comportamiento normal asociado con el dispositivo IoT (900) puede construirse a lo largo del tiempo en base a (...) los vectores de comportamiento (932) generados en la plataforma de monitoreo de salud en el dispositivo (910), vectores de comportamiento y / o modelos correspondientes a otros dispositivos en la red local de IoT (...) (Párr. 00102).
Almacenar un conjunto de reglas de seguridad que están asociadas con una condición esperada de al menos un dispositivo de IoT.	(...) Los umbrales u otros parámetros utilizados para detectar las anomalías pueden depender del contexto, ya que los umbrales de detección de anomalías u otros parámetros de detección de anomalías podrían reflejar condiciones normales o anormales en diferentes escenarios (...) (Párr. 00122).
Recibir los datos agregados del dispositivo de IoT desde al menos un dispositivo de IoT cuando dicho al menos un dispositivo de IoT	En el caso de uso del dispositivo de IoT de refrigerador mostrado en la FIG. 16, el bloque (1620) puede incluir comparar el comportamiento observado en el dispositivo de IoT del refrigerador con uno o más modelos que indican un consumo de

Oficio N° 7020 de 7 de mayo de 2021

Ref. Expediente N° NC2019/0004599

determina enviar los datos de IoT en respuesta a que se ha excedido un umbral basado en uno o más de los tipos de datos, en donde los datos agregados del dispositivo de IoT incluyen al menos dos tipos diferentes de datos de la pluralidad de dispositivos de IoT.	energía normal (o anormal), temperatura ambiente y valores de carga asociados con el dispositivo de IoT del refrigerador. (...) Como alternativa, en respuesta a la determinación en el bloque (1630) de que el valor asociado con la característica de comportamiento de consumo de energía excede el valor umbral, se pueden verificar una o más características de comportamiento adicionales para determinar si el consumo de energía indica una anomalía potencial que puede requerir servicio al cliente o una condición normal bajo las circunstancias (...) (Párr. 00129). En respuesta a los bloques (1630), (1640), (1650) que dan como resultado determinaciones respectivas de que el consumo de energía observado excede el valor umbral, la temperatura ambiente observada es normal o por debajo de lo normal, y la carga observada es normal o por debajo de lo normal, una condición anómala puede ser detectado e informado en el bloque (1670), que puede comprender la transmisión de los parámetros de comportamiento observados al servicio al cliente (...) y posiblemente también los valores de umbral en comparación con los parámetros de comportamiento observados (...) (Párr. 00130). En la arquitectura distribuida (1100) mostrada en la FIG. 11, el dispositivo de monitoreo siempre encendido (1110) puede recibir uno o más registros de acción (1122) de los dispositivos de observación (1112), (1114), los dispositivos de agregación (1116), (1118) y el monitor de tráfico de red (1120), en donde el dispositivo de monitoreo siempre encendido (1110) puede comprender un módulo de extracción de vectores de comportamiento (1130) configurado para mapear las características contenidas en los registros de acción (1122) en un espacio n-dimensional para extraer uno o más vectores de comportamiento (1132) que representan los comportamientos observados (...) (Párr. 00112). (...) En el vector de comportamiento ejemplar (932) que se muestra arriba, las características de consumo de energía, temperatura interna y uso de la CPU tienen valores precisos, mientras que la conectividad a Internet comprende un valor binario, por lo que las características de consumo de energía, temperatura interna y uso de la CPU tienen una granularidad más fina que la función de conectividad a Internet (...) (Párr. 00101).
Emplear al menos un procesador para comparar los datos agregados del dispositivo de IoT con el modelo configurable de dispositivo de IoT en cuanto a si se ha violado el conjunto de reglas de seguridad de tal manera que la comparación se evalua con base en una combinación de al menos dos tipos diferentes de datos de al menos dos de la pluralidad de dispositivos de IoT considerados en conjunto.	(...) En varias realizaciones, los nodos analizadores (1070)-(1072) pueden analizar los vectores de comportamiento agregados de acuerdo con comparaciones con modelos específicos de marcas, versiones, etc., asociados con los dispositivos que corresponden a los comportamientos observados, que pueden obtenerse de los fabricantes o otros repositorios adecuados, basados en vectores de comportamiento de todos los dispositivos en la red IoT (1000) y un modelo específico para la red IoT (1000) y / o entradas e interacciones de usuarios asociados con la red IoT (1000), etc. En consecuencia, en lugar de detectar las anomalías de comportamiento basándose en una sola característica, los nodos analizadores (1070)-(1072) pueden usar el aprendizaje automático para detectar las anomalías de comportamiento mediante la evaluación de los vectores de comportamiento en combinación con modelos que se construyen a lo largo del tiempo para indicar un comportamiento normal, en general estados ambientales, etc. (Párr. 00109). La FIG. 15 ilustra un método ejemplar para realizar análisis de comportamiento directo y / o indirecto en un entorno de IoT local para automatizar el servicio al cliente y las respuestas a incidentes de seguridad para remediar el comportamiento

Oficio N° 7020 de 7 de mayo de 2021

Ref. Expediente N° NC2019/0004599

	anómalo, de acuerdo con varios aspectos (Párr. 0029).
Enviar selectivamente una alerta con base en la comparación.	En diversas realizaciones, el módulo de análisis (1140) puede invocar uno o más actuadores (1170) para remediar una o más anomalías de comportamiento detectadas en los vectores de comportamiento analizados (1132) (...) (Párr. 00113).

De acuerdo con la tabla anterior, las características esenciales del método de la reivindicación 13 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 14: En la red IoT distribuida (1000) mostrada en la FIG. 10, los dispositivos configurados para operar en la función de observador comprenden altavoces exteriores (1012), (1014), altavoces interiores (1016), (1018), un termostato (1020), una lavadora (1022), un reloj (1024), una cafetera (1026), un altavoz de piso de la sala de estar (1028), un sistema de audio de estantería (1030), altavoces de cine en casa (1032), (1034) y un pomo de la puerta (1036), denominados colectivamente en el presente documento como nodos de observación (1012)-(1036). Además, los dispositivos configurados para operar en la función de agregador comprenden un refrigerador (1050) y un televisor (1052), denominados colectivamente en este documento como nodos de agregación (1050)-(1052), y los dispositivos configurados para operar en la función de analizador comprenden un teléfono inteligente (1070) y un enrutador inalámbrico o puerta de enlace doméstica (1072), denominada colectivamente en este documento como nodos analizadores (1070)-(1072) (...) (Párr. 00107). En la arquitectura distribuida (1100) mostrada en la FIG. 11, el dispositivo de monitoreo siempre encendido (1110) puede recibir uno o más registros de acción (1122) de los dispositivos de observación (1112), (1114), los dispositivos de agregación (1116), (1118) y el monitor de tráfico de red (1120) (...) (Párr. 00112).
- Reivindicación 15: (...) En el vector de comportamiento ejemplar (932) que se muestra arriba, las características de consumo de energía, temperatura interna y uso de la CPU tienen valores precisos, mientras que la conectividad a Internet comprende un valor binario, por lo que las características de consumo de energía, temperatura interna y uso de la CPU tienen una granularidad más fina que la función de conectividad a Internet (...) (Párr. 00101). (...) El dispositivo IoT (900) puede monitorear un entorno local asociado con el mismo (por ejemplo, un acelerómetro que puede medir la aceleración y la inclinación, un sensor de temperatura que puede medir la temperatura interna y / o ambiental, un fotosensor que puede detectar la luz, una antena que puede monitorear las señales inalámbricas locales, instrumentos que pueden detectar la actividad del procesador, la actividad de la red, etc.) (...) (Párr. 00099).
- Reivindicación 16: (...) En diversas realizaciones, los umbrales de detección de anomalías o los parámetros de detección de anomalías se pueden aprender a lo largo del tiempo y personalizarse según los requisitos específicos del usuario o los patrones de uso según el dispositivo, lo que puede garantizar que no se utilice un solo modelo para detectar todas las anomalías y, por lo tanto potencialmente aumentar las tasas de falsos positivos y / o las tasas de falsos negativos (...) (Párr. 00122).

Oficio N° 7020 de 7 de mayo de 2021

Ref. Expediente N° NC2019/0004599

Las reivindicaciones dependientes 14 a 16 tampoco cumplen con el requisito de novedad.

La reivindicación 17 consiste en: “Un método para la seguridad del internet de las cosas (IoT, por sus siglas en inglés), que comprende: (...)” (Radicado N° NC2019/0004599 del 19 de abril de 2021).

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

Características esenciales	D1
Emplear al menos un procesador para generar una solicitud de configuración, en donde la solicitud de configuración es una solicitud para cambiar un conjunto de reglas de seguridad a un conjunto ajustado de reglas de seguridad, en donde el conjunto ajustado de reglas de seguridad está asociado con una condición esperada de al menos un dispositivo de IoT.	(...) Un medio de almacenamiento ejemplar está acoplado al procesador de modo que el procesador pueda leer información y escribir información en el medio de almacenamiento (...) (Párr. 00143). (...) En diversas realizaciones, los umbrales de detección de anomalías o los parámetros de detección de anomalías se pueden aprender a lo largo del tiempo y personalizarse según los requisitos específicos del usuario o los patrones de uso según el dispositivo, lo que puede garantizar que no se utilice un solo modelo para detectar todas las anomalías y, por lo tanto potencialmente aumentar las tasas de falsos positivos y / o las tasas de falsos negativos (...) (Párr. 00122).
En donde el conjunto ajustado de reglas de seguridad se basa en una evaluación de los datos de IoT asociados con cada uno de la pluralidad de dispositivos de IoT.	(...) Los vectores de comportamiento (1132) generados en el módulo de extracción del vector de comportamiento (1130) se pueden proporcionar luego a un módulo de análisis (1140), que puede agregar los vectores de comportamiento (1132) para detectar una o más anomalías de comportamiento que podrían indicar posibles ataques maliciosos, mal funcionamiento o agotamiento en los dispositivos monitoreados u otras anomalías. (...) (Párr. 00112).
En donde los datos de IoT son datos agregados que son recibidos de al menos un dispositivo de IoT cuando dicho al menos un dispositivo de IoT determina enviar los datos de IoT en respuesta a que se ha excedido un umbral basado en uno o más de los tipos de datos y que incluyen al menos dos tipos diferentes de datos de la pluralidad de dispositivos de IoT de manera que la aplicación del conjunto ajustado de reglas de seguridad está basado en una combinación de al menos dos tipos diferentes de datos de al menos dos de la pluralidad de dispositivos de IoT considerados en conjunto.	En el caso de uso del dispositivo de IoT de refrigerador mostrado en la FIG. 16, el bloque (1620) puede incluir comparar el comportamiento observado en el dispositivo de IoT del refrigerador con uno o más modelos que indican un consumo de energía normal (o anormal), temperatura ambiente y valores de carga asociados con el dispositivo de IoT del refrigerador. (...) Como alternativa, en respuesta a la determinación en el bloque (1630) de que el valor asociado con la característica de comportamiento de consumo de energía excede el valor umbral, se pueden verificar una o más características de comportamiento adicionales para determinar si el consumo de energía indica una anomalía potencial que puede requerir servicio al cliente o una condición normal bajo las circunstancias (...) (Párr. 00129). En respuesta a los bloques (1630), (1640), (1650) que dan como resultado determinaciones respectivas de que el consumo de energía observado excede el valor umbral, la temperatura ambiente observada es normal o por debajo de lo normal, y la carga observada es normal o por debajo de lo normal, una condición anómala puede ser detectado e informado en el bloque (1670), que puede comprender la transmisión de los parámetros de comportamiento observados al servicio al cliente (...) y posiblemente también los valores de umbral en comparación con los parámetros de comportamiento observados (...) (Párr. 00130). En la arquitectura distribuida (1100) mostrada en la FIG. 11, el dispositivo de monitoreo siempre encendido (1110) puede recibir uno o más registros de acción (1122) de los dispositivos de observación (1112), (1114), los dispositivos de agregación (1116), (1118) y el monitor de tráfico de red (1120), en donde el dispositivo de monitoreo siempre encendido (1110) puede comprender un módulo de extracción de vectores de comportamiento (1130) configurado para mapear las

Oficio N° 7020 de 7 de mayo de 2021

Ref. Expediente N° NC2019/0004599

	características contenidas en los registros de acción (1122) en un espacio n-dimensional para extraer uno o más vectores de comportamiento (1132) que representan los comportamientos observados (...) (Párr. 00112). (...) En el vector de comportamiento ejemplar (932) que se muestra arriba, las características de consumo de energía, temperatura interna y uso de la CPU tienen valores precisos, mientras que la conectividad a Internet comprende un valor binario, por lo que las características de consumo de energía, temperatura interna y uso de la CPU tienen una granularidad más fina que la función de conectividad a Internet (...) (Párr. 00101).
Enviar la solicitud de configuración a un concentrador de IoT.	(...) En diversas realizaciones, los umbrales de detección de anomalías o los parámetros de detección de anomalías se pueden aprender a lo largo del tiempo y personalizarse según los requisitos específicos del usuario o los patrones de uso según el dispositivo (...) (Párr. 00122).
Recibir una alerta del concentrador de IoT cuando el concentrador de IoT determina que se infringió el conjunto ajustado de reglas de seguridad.	En diversas realizaciones, el módulo de análisis (1140) puede invocar uno o más actuadores (1170) para remediar una o más anomalías de comportamiento detectadas en los vectores de comportamiento analizados (1132) (...) (Párr. 00113).

De acuerdo con la tabla anterior, las características esenciales del método de la reivindicación 17 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 18: (...) Los vectores de comportamiento (1132) generados en el módulo de extracción del vector de comportamiento (1130) se pueden proporcionar luego a un módulo de análisis (1140), que puede agregar los vectores de comportamiento (1132) para detectar una o más anomalías de comportamiento que podrían indicar posibles ataques maliciosos, mal funcionamiento o agotamiento en los dispositivos monitoreados u otras anomalías. (...) (Párr. 00112). En la red IoT distribuida (1000) mostrada en la FIG. 10, los dispositivos configurados para operar en la función de observador comprenden altavoces exteriores (1012), (1014), altavoces interiores (1016), (1018), un termostato (1020), una lavadora (1022), un reloj (1024), una cafetera (1026), un altavoz de piso de la sala de estar (1028), un sistema de audio de estantería (1030), altavoces de cine en casa (1032), (1034) y un pomo de la puerta (1036), denominados colectivamente en el presente documento como nodos de observación (1012)-(1036). Además, los dispositivos configurados para operar en la función de agregador comprenden un refrigerador (1050) y un televisor (1052), denominados colectivamente en este documento como nodos de agregación (1050)-(1052), y los dispositivos configurados para operar en la función de analizador comprenden un teléfono inteligente (1070) y un enrutador inalámbrico o puerta de enlace doméstica (1072), denominada colectivamente en este documento como nodos analizadores (1070)-(1072) (...) (Párr. 00107).
- Reivindicación 19: En el vector de comportamiento ejemplar (932) que se muestra arriba, las características de consumo de energía, temperatura interna y uso de la CPU tienen valores precisos, mientras que la conectividad a Internet comprende un valor binario, por lo que las características de consumo de energía, temperatura interna y uso de la CPU tienen una granularidad más fina que la función de conectividad a Internet (...) (Párr. 00101). (...) El dispositivo IoT (900) puede monitorear un entorno local asociado con el mismo (por ejemplo, un acelerómetro

Oficio N° 7020 de 7 de mayo de 2021

Ref. Expediente N° NC2019/0004599

que puede medir la aceleración y la inclinación, un sensor de temperatura que puede medir la temperatura interna y / o ambiental, un fotosensor que puede detectar la luz, una antena que puede monitorear las señales inalámbricas locales, instrumentos que pueden detectar la actividad del procesador, la actividad de la red, etc.) (...) (Párr. 0099).

- Reivindicación 20: (...) Los comportamientos de uso de un dispositivo IoT que es un termostato puede incluir a qué temperaturas está configurado el termostato en momentos específicos. En otro ejemplo, los comportamientos de uso de un dispositivo IoT que es un televisor inteligente puede incluir qué medios se ven en momentos específicos a través del televisor inteligente y con qué servidores interactúa el televisor inteligente en momentos específicos (...) (Párr. 0046).

Las reivindicaciones dependientes 18 a 20 tampoco cumplen con el requisito de novedad.

6. 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	WO2016140912	1 a 20	Novedad

7. Respuesta a los argumentos del solicitante

El solicitante argumenta que “(...) *Primero se indica que las reivindicaciones 1, 13, y 17 se modificaron con el objetivo de que sean aún más claros su novedad y nivel inventivo donde ahora incluyen la siguiente característica que no son divulgadas ni sugeridas por el documento D1:*

- datos de IoT que son recibidos “cuando dicho al menos un dispositivo de IoT determina enviar los datos de IoT en respuesta a que se ha excedido un umbral basado en uno o más de los tipos de datos” (...).”

Se aclara que el documento D1 menciona que se puede comparar el comportamiento observado en el dispositivo de IoT del refrigerador con uno o más modelos que indican un consumo de energía normal (o anormal), temperatura ambiente y valores de carga asociados con el dispositivo, donde en respuesta a la determinación en el bloque (1630) de que el valor asociado con la característica de comportamiento de consumo de energía excede el valor umbral, se pueden verificar una o más características de comportamiento adicionales para determinar si el consumo de energía indica una anomalía potencial que puede requerir servicio al cliente o una condición normal bajo las circunstancias (Párr. 00129). Asimismo, D1 afirma que en respuesta a los bloques (1630), (1640), (1650) que dan como resultado determinaciones respectivas de que el consumo de energía observado excede el valor umbral, la temperatura ambiente observada es normal o por debajo de lo normal, y la carga observada es normal o por debajo de lo normal, una condición anómala puede ser detectado e informado en el bloque (1670), que puede comprender la transmisión de los parámetros de comportamiento observados al servicio al cliente y posiblemente también los valores de umbral en comparación con los parámetros de comportamiento observados (Párr. 00130). Por lo tanto, el documento D1 si realiza la transmisión de datos de un dispositivo IoT a un servicio externo a dicho dispositivo cuando se ha detectado que los parámetros de comportamiento observados exceden los valores de umbral definidos



Oficio N° 7020 de 7 de mayo de 2021

Ref. Expediente N° NC2019/0004599

para los mismos, tal como sucede en la característica reclamada para la solicitud de patente, afectando así la novedad de la misma.

El solicitante afirma que “(...) Si bien dichos dos métodos alternativos permiten identificar cualquier amenaza para los dispositivos de IoT de forma satisfactoria como en la presente solicitud, ambos métodos alternativos descritos en el documento D1 son, sin embargo, menos eficientes computacionalmente que la solución proporcionada en la presente solicitud (...)”.

Con respecto a la característica de eficiencia computacional ofrecida por el aparato y métodos reclamados, cabe indicar que estas características no se encuentran divulgadas en las reivindicaciones del capítulo estudiado, por lo tanto, no hacen parte del estudio de novedad realizado. Resulta del caso señalar que, el artículo 30 de la Decisión 486 señala que las reivindicaciones deben ser claras y concisas y contener todas las características técnicas esenciales de la invención.

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.

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° 7020 de 7 de mayo de 2021

Ref. Expediente N° NC2019/0004599

INFORME DE BÚSQUEDA
EXAMEN DE PATENTABILIDAD

Solicitud No.		Examen de patentabilidad							
NC2019/0004599		1°		2°		3°	X	Revoca	
Solicitud Internacional No.		Fecha solicitud internacional: (DD/MM/AÑO)							
PCT/US2017/058926		30 de octubre de 2017							
Fecha de determinación estado de la técnica (DD/MM/AÑO)				Prioridad			Presentación		
04/11/2016				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 20
Palabras clave utilizadas	IoT, Security, Firewall, Rules, Policies, IoT Hub, Data Collection, Alert, Anomaly Detection, Cyber Attack, Physical Attack, Attack Detection, Environmental Data, Internal State Data.
Clasificaciones utilizadas para la búsqueda	CIP: H04L 29/06, G06F 21/55, H04W 4/00, H04L 12/26

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	14266862	29/12/2014	-	-	A
WO	WO2016140912	09/09/2016	1 a 20	1 Resumen, Párr. 00143, Párr. 00122, Párr. 00102, Párr. 00101, Párr. 00112, Párr. 00109, Párr. 00113, Párr. 00130, Párr. 00129. 2 Párr. 00122. 3 y 4 Párr. 00107, Párr. 00112. 5 Párr. 00128. 6 Párr. 00037. 7 Párr. 00107. 8 y 9 Párr. 00101, Párr. 0099. 10 Párr. 0046. 11 Párr. 0005. 12 Párr. 00113. 13 Párr. 00122, Párr. 00102, Párr. 00112, Párr. 00101, Párr. 00109, Párr. 00113, Párr. 00130, Párr. 00129. 14 Párr. 00107, Párr. 00112. 15	X

Oficio N° 7020 de 7 de mayo de 2021

Ref. Expediente N° NC2019/0004599

				Párr. 00101, Pár. 0099. 16 Párr. 00122. 17 Párr. 00143, Párr. 00122, Párr. 00112, Párr. 00109, Párr. 00101, Párr. 00122, Párr. 00113, Párr. 00130, Párr. 00129. 18 Párr. 00112, Párr. 00107. 19 Párr. 00101, Párr. 0099. 20 Párr. 0046.	
US	US20160212099	21/07/2016	-	-	A
Patbase	US2015019553	15/01/2015	-	-	A
EPOQUENET	US2015058914	26/02/2015	-	-	A
(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: (03/05/2021)					
Examinador: CARLOS EDUARDO GUEVARA NICHROY					