

REPÚBLICA DE COLOMBIA
SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO

Resolución N° 55560

Ref. Expediente N° NC2019/0004599

Por la cual se deniega una Patente de Invención

EL SUPERINTENDENTE DE INDUSTRIA Y COMERCIO
en ejercicio de sus facultades legales, en especial de las conferidas en el numeral 26 del artículo 3° del Decreto 4886 de 2011, y

CONSIDERANDO

PRIMERO: Que mediante escrito radicado en esta Superintendencia el 3 de mayo de 2019, con el N° NC2019/0004599, por LLC MICROSOFT TECHNOLOGY LICENSING, entró a fase nacional la solicitud de patente de invención titulada “SERVICIO DE SEGURIDAD DEL INTERNET DE LAS COSAS”, que corresponde a la solicitud internacional que corresponde a la solicitud internacional PCT/US2017/058926 del 30 de octubre de 2017.

SEGUNDO: Que la solicitud fue publicada en la Gaceta de la Propiedad Industrial N° 859 el 10 de mayo de 2019, sin que se hubieran presentado oposiciones por parte de terceros.

TERCERO: Que realizado el examen de fondo mediante Oficio N° 7020, notificado el 10 de mayo de 2021, se requirió al solicitante en los términos del artículo 45 de la Decisión 486 de la Comisión de la Comunidad Andina para que presentara respuesta a las observaciones de carácter técnico, relacionadas con la patentabilidad o cumplimiento de los requisitos establecidos por esta Decisión para la concesión de la patente.

CUARTO: Que el solicitante mediante escrito radicado bajo el N° NC2019/0004599 el 3 de agosto de 2021, respondió oportunamente el requerimiento formulado y presentó las reivindicaciones 1 a 20 que reemplazan las originalmente presentadas. Se acepta este último capítulo reivindicatorio presentado, comoquiera que se ajusta a las prescripciones contenidas en el artículo 34 de la Decisión 486.

QUINTO: Que en virtud de lo dispuesto en el artículo 14 de la Decisión 486 expedida por la Comisión de la Comunidad Andina *“Los países miembros otorgarán patentes para las invenciones, sean de producto o de procedimiento, en todos los campos de la tecnología, siempre que sean nuevas, tengan nivel inventivo y sean susceptibles de aplicación industrial”*.

SEXTO: Que en el presente caso las reivindicaciones 1 a 20 incluidas en el radicado bajo el N° NC2019/0004599 el 3 de agosto de 2021, no cumplen los requisitos indicados. Lo anterior, de acuerdo con las siguientes consideraciones:

6.1 Objeto de la invención

El problema técnico planteado 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.

Resolución N° 55560

Ref. Expediente N° NC2019/0004599

Para resolver este problema técnico, la solicitud 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.

6.2 Determinación del estado de la técnica

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 encontró el siguiente documento que anticipa 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 u 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)

6.3 Novedad (Art 16 Decisión 486)

Según lo dispuesto en el artículo 16 de la Decisión 486: *“Una invención se considerará nueva cuando no está comprendida en el estado de la técnica.*

El estado de la técnica comprenderá todo lo que haya sido accesible al público por una descripción escrita u oral, utilización, comercialización o cualquier otro medio antes de la fecha de presentación de la solicitud de patente o, en su caso, de la prioridad reconocida”.

En el presente caso, el aparato reclamado en la solicitud no es nuevo, teniendo en cuenta que la reivindicación 1 está referida a: *“Un aparato para la seguridad del internet de las cosas (IoT, por sus siglas en inglés), que comprende: (...)”* (Radicado N° NC2019/0004599 del 3 de agosto de 2021).

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

Resolución N° 55560

Ref. Expediente N° NC2019/0004599

La siguiente tabla presenta la comparación entre las características técnicas esenciales de la solicitud estudiada, mencionadas en la reivindicación 1, y las reveladas en el documento D1 que representa el estado de la técnica:

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

Características esenciales	D1
Un concentrador de IoT (351) 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 (...). (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 (351) realice las acciones, que incluyen:	(...) 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).
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 (591) 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 (341).	(...) 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 (...). (Párr. 00101).
Recibir datos de IoT (592) asociados con al menos un dispositivo de IoT (341) 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 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. (...) 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 (...) (Párr. 00129). (...) Comprender la transmisión de los parámetros de comportamiento observados al servicio al cliente (...) (Párr. 00130).
En donde los datos de IoT son datos agregados que	(...) En el vector de comportamiento ejemplar (932) que se muestra arriba, las características de consumo de energía, temperatura interna y

Resolución N° 55560

Ref. Expediente N° NC2019/0004599

incluyen al menos dos tipos diferentes de datos.	uso de la CPU tienen valores precisos (...). (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 (593) 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 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). (...) La plataforma de servicio al cliente (1410) puede recibir uno o más registros de acción de los dispositivos IoT del observador (1412), (1414) además del contexto local relevante y/o información del entorno de los dispositivos IoT informativos (1416), (1418), (1420) (...). Los vectores de comportamiento se pueden proporcionar (...) a un módulo de análisis (1440), en el que el módulo de análisis (1440) puede agregar los vectores de comportamiento para detectar una o más anomalías de comportamiento que podrían indicar posibles ataques maliciosos, mal funcionamiento o quemaduras en los dispositivos monitoreados, u otras anomalías (...). (Párr. 0121).
Enviar selectivamente una alerta (594) con base en la determinación.	(...) El módulo de análisis (940) puede notificar a otro agregador y/o nodo analizador en la red local de IoT para solicitar asistencia para remediar las anomalías de comportamiento (944) (...). (Párr. 00103).

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

Resolución N° 55560

Ref. Expediente N° NC2019/0004599

dispositivos de agregación (1116), (1118) y el monitor de tráfico de red (1120) (...) (Párr. 00112).

- 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



Resolución N° 55560

Ref. Expediente N° NC2019/0004599

pueden detectar la actividad del procesador, la actividad de la red, etc.) (...) (Párr. 0099).

- 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.

Según lo dispuesto en el artículo 16 de la Decisión 486: *“Una invención se considerará nueva cuando no está comprendida en el estado de la técnica.*

El estado de la técnica comprenderá todo lo que haya sido accesible al público por una descripción escrita u oral, utilización, comercialización o cualquier otro medio antes de la fecha de presentación de la solicitud de patente o, en su caso, de la prioridad reconocida”.

En el presente caso, el método reclamado en la solicitud no es nuevo, teniendo en cuenta que la reivindicación 13 está referida a: *“Un método para la seguridad del internet de las cosas (IoT, por sus siglas en inglés), que comprende: (...)”* (Radicado N° NC2019/0004599 del 3 de agosto de 2021).

La siguiente tabla presenta la comparación entre las características técnicas esenciales de la solicitud estudiada, mencionadas en la reivindicación 13, y las reveladas en el documento D1 que representa el estado de la técnica:

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.	(...) 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 (591) un conjunto de reglas de seguridad que están asociadas con una	(...) 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

Resolución N° 55560

Ref. Expediente N° NC2019/0004599

condición esperada de al menos un dispositivo de IoT (341).	podrían reflejar condiciones normales o anormales en diferentes escenarios (...). (Párr. 00122).
Recibir los datos agregados del dispositivo de IoT (592) desde al menos un dispositivo de IoT (341) cuando dicho al menos un dispositivo de IoT (341) 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 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. (...) 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 (...). (Párr. 00129). (...) Comprender la transmisión de los parámetros de comportamiento observados al servicio al cliente (...) (Párr. 00130).
En donde los datos agregados del dispositivo de IoT incluyen al menos dos tipos diferentes de datos de la pluralidad de dispositivos de IoT.	(...) 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 (...). (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 evalúa 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 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). (...) La plataforma de servicio al cliente (1410) puede recibir uno o más registros de acción de los dispositivos IoT del observador (1412), (1414) además del contexto local relevante y/o información del entorno de los dispositivos IoT informativos (1416), (1418), (1420) (...). Los vectores de comportamiento se pueden proporcionar (...) a un módulo de análisis (1440), en el que el módulo de análisis (1440) puede agregar los vectores de comportamiento para detectar una o más anomalías de comportamiento que podrían indicar posibles ataques maliciosos, mal funcionamiento o quemaduras en los dispositivos monitoreados, u otras anomalías (...). (Párr. 0121).
Enviar selectivamente una alerta (594) con base en la comparación.	(...) El módulo de análisis (940) puede notificar a otro agregador y/o nodo analizador en la red local de IoT para solicitar asistencia para remediar las anomalías de comportamiento (944) (...). (Párr. 00103).

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

Resolución N° 55560

Ref. Expediente N° NC2019/0004599

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).

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

Según lo dispuesto en el artículo 16 de la Decisión 486: *“Una invención se considerará nueva cuando no está comprendida en el estado de la técnica.*

El estado de la técnica comprenderá todo lo que haya sido accesible al público por una descripción escrita u oral, utilización, comercialización o cualquier otro medio antes de la fecha de presentación de la solicitud de patente o, en su caso, de la prioridad reconocida”.

En el presente caso, el método reclamado en la solicitud no es nuevo, teniendo en cuenta que la reivindicación 17 está referida a: *“Un método para la seguridad del internet de las cosas (IoT, por sus siglas en inglés), que comprende: (...)”* (Radicado N° NC2019/0004599 del 3 de agosto de 2021).

La siguiente tabla presenta la comparación entre las características técnicas esenciales de la solicitud estudiada, mencionadas en la reivindicación 17, y las reveladas en el documento D1 que representa el estado de la técnica:



Resolución N° 55560

Ref. Expediente N° NC2019/0004599

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 (423), en donde la solicitud de configuración (423) 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 (341).	(...) 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). (...) 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).
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 (341, 342, 343).	(...) 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 (341) cuando dicho al menos un dispositivo de IoT (341) 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. (...) 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 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 (...). (Párr. 00101).
Enviar la solicitud de configuración a un concentrador de IoT (351).	(...) 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 (351) cuando el concentrador de IoT determina que se infringió el conjunto ajustado de reglas de seguridad.	(...) El módulo de análisis (940) puede notificar a otro agregador y/o nodo analizador en la red local de IoT para solicitar asistencia para remediar las anomalías de comportamiento (944) (...). (Párr. 00103).

Resolución N° 55560

Ref. Expediente N° NC2019/0004599

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 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 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.

6.4 Respuesta a los argumentos del solicitante



Resolución N° 55560

Ref. Expediente N° NC2019/0004599

El solicitante afirma que “(...) La solicitud de la presente invención requiere de las siguientes características que no son divulgadas en conjunto por el documento D1:

- recibir datos de IoT (592) asociados con al menos un dispositivo de IoT (341) 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; (...).”

Se aclara que el documento D1 menciona que 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, 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) y posteriormente, comprender la transmisión de los parámetros de comportamiento observados al servicio al cliente (Párr. 00130). Por lo tanto, D1 muestra que se realiza la transmisión de información al servicio al cliente que en este caso corresponde con el dispositivo IoT concentrador, donde dicha transmisión se realiza cuando el dispositivo IoT (refrigerador) determina que el valor sus las características de comportamiento (consumo de energía, temperatura ambiente y valores de carga) han superado un valor umbral, por lo tanto, D1 si muestra la recepción de información por parte del dispositivo IoT concentrador cuando un dispositivo IoT determina que se ha excedido un umbral basado en uno o más tipos de datos agregados, que incluyen al menos dos tipos diferentes de datos, para el caso de D1 estos datos son el consumo de energía, la temperatura ambiente y los valores de carga, de esta manera, D1 anticipa las características reclamadas en la presente solicitud.

El solicitante asegura que “(...) La solicitud de la presente invención requiere de las siguientes características que no son divulgadas en conjunto por el documento D1: (...)

- 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 (593) 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; (...).”

Se aclara que el documento D1 menciona 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). Posteriormente, D1 muestra que la plataforma de servicio al cliente (1410) puede recibir uno o más registros de acción de los dispositivos IoT del observador (1412), (1414) además del contexto local relevante y/o información del entorno de los dispositivos IoT informativos (1416), (1418), (1420) y proporcionar los vectores de comportamiento a un módulo de análisis (1440), en el que el módulo de análisis (1440) puede agregar los vectores de



Resolución N° 55560

Ref. Expediente N° NC2019/0004599

comportamiento para detectar una o más anomalías de comportamiento que podrían indicar posibles ataques maliciosos, mal funcionamiento o quemaduras en los dispositivos monitoreados, u otras anomalías (Párr. 00121). Por lo tanto, D1 revela que existe una plataforma de servicio al cliente que como se mencionó anteriormente corresponde al dispositivo concentrador IoT reclamado, donde se recibe información por parte de los dispositivos IoT una vez dichos dispositivos han determinado que su comportamiento excede un valor umbral, con la información recibida, la plataforma de servicio al cliente utiliza un módulo de análisis donde se detectan anomalías del comportamiento de los dispositivos IoT, por consiguiente y contrario a lo afirmado por el solicitante, D1 si realiza un procesamiento adicional en el concentrador IoT con la información recibida de los dispositivos IoT cuando estos determinan que sus características superan un valor umbral determinado, afectando así la novedad de la solicitud.

El solicitante argumenta que “(...) *La solicitud de la presente invención requiere de las siguientes características que no son divulgadas en conjunto por el documento D1: (...)* - *enviar selectivamente una alerta (594) con base en la determinación (...)*”.

Se aclara que el documento D1 menciona que el módulo de análisis (940) puede notificar a otro agregador y/o nodo analizador en la red local de IoT para solicitar asistencia para remediar las anomalías de comportamiento (944) (Párr. 00103). Por lo tanto, D1 revela que el módulo de análisis notifica a los elementos de la red IoT para solicitar asistencia para solucionar las diferentes anomalías encontradas, anticipando de esta manera el envío de alertas con base en la determinación realizada reclamado en la presente solicitud de patente.

El solicitante menciona que “(...) *Nótese que la invención que se reclama en la presente solicitud, a diferencia de lo divulgado en el documento D1, requiere de dos determinaciones una realizada en el dispositivo IoT y otra en el en el concentrador IoT correspondientes a las siguiente:*

- *determinar, en el dispositivo IoT, si ha excedido un umbral basado en uno o más de los tipos de datos para que el dispositivo IoT envíe los datos, que son recibido en el concentrador IoT, para permitir una segunda determinación; y*
- *determinar, en el concentrador 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 (593) para el dispositivo IoT (...)*”.

El solicitante afirma que “(...) *el documento D1, no menciona una segunda determinación, y mucho menos que dicha segunda determinación se realice con datos enviados por los dispositivos IoT (y recibidos en el concentrador IoT) en consecuencia de la primera determinación como lo requiere la invención que se reclama.*

(...) El documento D1 no menciona ni sugiere que dicho servicio al cliente haga una segunda determinación y mucho menos una determinación de si se infringió un conjunto de reglas de seguridad para el dispositivo IoT con base en los datos de IoT y en el modelo de dispositivo de IoT.

(...) todo los párrafos se refieren a la misma determinación y no, a determinaciones diferentes como lo requiere la presente invención, por lo tanto, dichos párrafos, ni nada en el documento D1, divulgan o sugieren las dos determinaciones requerida en la invención de la presente solicitud (...)”.

Resolución N° 55560

Ref. Expediente N° NC2019/0004599

Se aclara que el documento D1 menciona que 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, 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). Posteriormente, el documento D1 muestra 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). Finalmente, D1 enseña que la plataforma de servicio al cliente (1410) puede recibir uno o más registros de acción de los dispositivos IoT del observador (1412), (1414) además del contexto local relevante y/o información del entorno de los dispositivos IoT informativos (1416), (1418), (1420) y proporcionar los vectores de comportamiento a un módulo de análisis (1440), en el que el módulo de análisis (1440) puede agregar los vectores de comportamiento para detectar una o más anomalías de comportamiento que podrían indicar posibles ataques maliciosos, mal funcionamiento o quemaduras en los dispositivos monitoreados, u otras anomalías (Párr. 00121).

Teniendo en cuenta los párrafos anteriores, resulta evidente que D1 si revela dos determinaciones como lo requiere la presente solicitud de patente, la primera determinación ocurre cuando el dispositivo IoT (refrigerador) determina que las características de su comportamiento (consumo de energía, temperatura ambiente y valores de carga) superan un umbral predeterminado, posterior a esta determinación se envía la información al servicio al cliente que opera como un concentrador IoT. Cuando la plataforma de servicio al cliente recibe la información de los dispositivos IoT, utiliza un módulo de análisis para detectar una o más anomalías de comportamiento que podrían indicar posibles ataques maliciosos, mal funcionamiento o quemaduras de los dispositivos IoT, este procedimiento corresponde a la segunda determinación que claramente es realizada por la plataforma de servicio al cliente (dispositivo agregador). Por lo tanto, se reitera que D1 si realiza una secuencia de dos determinaciones tal como lo requiere la presente solicitud de patente, la primera realizada en los propios dispositivos IoT y la segunda realizada en la plataforma de servicio al cliente o dispositivo concentrador IoT donde finalmente se determina la anomalía, anticipando así las características reclamadas.

SÉPTIMO: Que de acuerdo con la modificación presentada por el solicitante en el escrito radicado bajo el N° NC2019/0004599 el 15 de septiembre de 2020 y teniendo en cuenta el objeto de la solicitud, se modifica el título de la invención el cual quedará de la siguiente manera: “APARATO Y MÉTODOS PARA SERVICIO DE SEGURIDAD DEL INTERNET DE LAS COSAS”.

En conclusión, teniendo en cuenta que los argumentos del solicitante no desvirtúan de manera alguna las objeciones a la patentabilidad ya sustentadas, el Superintendente de Industria y Comercio,

Resolución N° 55560

Ref. Expediente N° NC2019/0004599

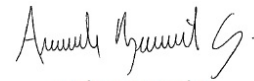
RESUELVE

ARTÍCULO PRIMERO: Denegar la patente de invención a la creación titulada “APARATO Y MÉTODOS PARA SERVICIO DE SEGURIDAD DEL INTERNET DE LAS COSAS”.

ARTÍCULO SEGUNDO: Notificar el contenido de la presente resolución a LLC MICROSOFT TECHNOLOGY LICENSING, advirtiéndole que contra ella procede el recurso de reposición, ante el Superintendente de Industria y Comercio, el cual podrá ser interpuesto en el momento de la notificación o dentro de los diez (10) días hábiles siguientes a ella.

NOTIFÍQUESE Y CÚMPLASE

Dada en Bogotá D.C., el 30 de agosto de 2021



ANDRÉS BARRETO GONZÁLEZ
SUPERINTENDENTE DE INDUSTRIA Y COMERCIO

Firmado digitalmente
por: ANDRÉS
BERNARDO BARRETO
GONZÁLEZ
Fecha: 2021.08.30
17:06:05 COT
Razón: Validez jurídica.
Ubicación: Bogotá,
Colombia.

