

REPÚBLICA DE COLOMBIA
SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO

Oficio N° 10562 de 8 de julio de 2022

Ref. Expediente N° NC2019/0004599

Señores
LLC MICROSOFT TECHNOLOGY LICENSING

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

NUMERO DE SOLICITUD INTERNACIONAL: PCT/US2017/058926

FECHA DE PRESENTACIÓN INTERNACIONAL: 30 de octubre de 2017.

PRIORIDAD: 4/11/2016, US (ESTADOS UNIDOS DE AMÉRICA), 15/344,461

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

Revisada la modificación a la solicitud objeto de estudio, la cual fue radicada el 24 de mayo de 2022 bajo el número NC2019/0004599, y teniendo en cuenta lo señalado en el artículo 34 de la Decisión 486 de 2000 de la Comisión de la Comunidad Andina, esta oficina acepta las modificaciones presentadas por ajustarse a los requisitos legales.

2. Objeto de la invención

El problema 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.

Para resolver dicho problema técnico, la solicitud en estudio plantea 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. Reivindicaciones estudiadas

El presente estudio se basa en el capítulo reivindicatorio presentado el 24 de mayo de 2022.

4. 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 encontraron los siguientes documentos que anticipan el objeto de esta solicitud:

Oficio N° 10562 de 8 de julio de 2022

Ref. Expediente N° NC2019/0004599

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
D2	US20150163121	“Distributed monitoring, evaluation, and response for multiple devices”	11 de junio de 2015

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)

D2² divulga sistemas y métodos para el monitoreo de dispositivos, dichos dispositivos pueden incluir dispositivos de comunicaciones móviles, dispositivos sésiles (como parte de IoT (Internet de las cosas)) y otros dispositivos informáticos o de detección. En una implementación específica, los datos se recopilan de un conjunto de dispositivos informáticos. Los datos están asociados con los dispositivos, programas de aplicaciones móviles (apps), aplicaciones web, usuarios o combinaciones de estos (Párr. 0005).

5. Examen de Patentabilidad

De acuerdo con lo establecido en el artículo 14 de la Decisión 486 de 2000 de la Comisión de la Comunidad Andina, en el cual se establecen los requisitos de patentabilidad objeto de la solicitud en estudio, esta Oficina presenta a continuación el análisis de los requisitos de patentabilidad.

5.1. Nivel Inventivo

Teniendo en cuenta lo señalado en el artículo 18 de la Decisión 486 de 2000 de la Comisión de la Comunidad Andina, la reivindicación independiente 1 (NC2019/0004599 del 24 de mayo de 2022) refiere a: “*Un aparato para la seguridad del internet de las cosas (IoT, por sus siglas en inglés), que comprende: (...)*”. A continuación, se presenta la tabla comparativa entre el objeto reivindicado y los documentos encontrados en el estado de la técnica:

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

¹<https://patents.google.com/patent/WO2016140912A1/en?q=WO2016140912>
²<https://patents.google.com/patent/US20150163121A1/en?q=US2015163121>

Oficio N° 10562 de 8 de julio de 2022

Ref. Expediente N° NC2019/0004599

CARACTERÍSTICAS ESENCIALES	D1	D2
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).	Un servidor de recopilación de observaciones puede recibir los datos recopilados del dispositivo D y el dispositivo de red R (...). (Párr. 0275). (...) Una constelación personal que incluye (...) dispositivos sésiles que forman parte del IoT (Internet de las cosas) del usuario (...). (Párr. 0276).
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).	Una versión binaria, ejecutable por máquina, del software útil para practicar las técnicas descritas en esta solicitud puede almacenarse o residir en RAM o memoria caché (...). (Párr. 0049).
Y 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).	(...) Un sistema informático podría incluir más de un procesador (es decir, un sistema multiprocesador, que puede permitir el procesamiento paralelo de información) (...). (Párr. 0046).
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).	El método puede incluir además generar un modelo de características para un programa de aplicación específico en la pluralidad de dispositivos (...). (Párr. 0015).
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 análisis incluye una evaluación de reglas. Las reglas pueden ser para eventos específicos o frecuencia de eventos o para eventos o recuento o volumen o solo si son anómalos para el usuario (...). (Párr. 0184).
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).	(...) El servidor de análisis aplica técnicas de aprendizaje automático para evaluar los datos recopilados, establecer las normas e identificar anomalías. El aprendizaje puede ser no supervisado, semisupervisado o supervisado, pero el primero es generalmente el caso. (Párr. 0185).
Recibir datos de IoT (592) asociados con al menos un dispositivo de IoT (341) 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	No se menciona.

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.	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 incluyen al menos dos tipos diferentes de datos.	(...) 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).	No se menciona.
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).	No se menciona.
Y 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).	(...) Las respuestas pueden incluir notificaciones y alertas de un usuario, administrador o analista (...). (Párr. 0008).
En donde la determinación de si se infringió el conjunto	(...) Reportar la información de comportamiento observada en el	No se menciona.

Oficio N° 10562 de 8 de julio de 2022

Ref. Expediente N° NC2019/0004599

de reglas de seguridad (593) para el dispositivo IoT, la cual se basa en los datos IoT ya recibidos y ocurre a continuación después de recibir dichos datos IoT.	dispositivo IoT a una entidad de servicio al cliente en respuesta a la determinación de que la información de comportamiento observada en el dispositivo IoT indica un comportamiento anómalo. (Reiv. 5).	
Depende de otros factores a los utilizados en la determinación de enviar los datos de IoT en respuesta a que se ha excedido el umbral.	No se menciona.	(...) El aumento de la supervisión permite la recopilación de datos adicionales antes de tomar una determinación final sobre la existencia o no de actividad maliciosa (...). (Párr. 0233).

D1 es considerado como el estado de la técnica más cercano a la invención definida en la reivindicación 1, ya que divulga un aparato para monitorear el estado del dispositivo de Internet de las cosas (IoT) (...) (Reiv. 11).

La diferencia entre la invención definida entre la reivindicación 1 y el aparato divulgado en D1, consiste en que la invención incluye la determinación de si se infringió el conjunto de reglas de seguridad para el dispositivo IoT en función de otros factores a los utilizados en la determinación de enviar los datos de IoT en respuesta a que se ha excedido el umbral.

El efecto que se logra al incluir específicamente la determinación de si se infringió el conjunto de reglas de seguridad para el dispositivo IoT en función de otros factores a los utilizados en la determinación de enviar los datos de IoT en respuesta a que se ha excedido el umbral es garantizar un nivel alto de seguridad para los dispositivos IoT de una manera más eficiente.

Por lo tanto, el problema técnico objetivo que pretende resolver esta invención se puede formular así: ¿cómo modificar el aparato divulgado en D1 para garantizar un nivel alto de seguridad para los dispositivos IoT de una manera más eficiente?.

Sin embargo, el incluir la determinación de si se infringió el conjunto de reglas de seguridad para el dispositivo IoT en función de otros factores a los utilizados en la determinación de enviar los datos de IoT en respuesta a que se ha excedido el umbral para garantizar un nivel alto de seguridad para los dispositivos IoT de una manera más eficiente, ya está divulgado en D2 que se refiere a que un mayor monitoreo puede ser apropiado cuando el sistema tiene sospechas de actividad maliciosa, donde el aumento de la supervisión permite la recopilación de datos adicionales antes de tomar una determinación final sobre la existencia o no de actividad maliciosa (Párr. 0233).

En consecuencia, la persona normalmente versada en la materia estaría motivada a incluir la determinación de si se infringió el conjunto de reglas de seguridad para el dispositivo IoT en función de otros factores a los utilizados en la determinación de enviar los datos de IoT en respuesta a que se ha excedido el umbral del D2 en el aparato de D1, para así llegar al objeto de la reivindicación 1. Por lo cual se considera obvia.

Así mismo, D1 divulga las características de las reivindicaciones dependientes de la siguiente manera:

- 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

Oficio N° 10562 de 8 de julio de 2022

Ref. Expediente N° NC2019/0004599

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).

- 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



Oficio N° 10562 de 8 de julio de 2022

Ref. Expediente N° NC2019/0004599

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. 00099).

- 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 no mencionan alguna característica que, junto con las características de la reivindicación independiente, aporte nivel inventivo al aparato de la reivindicación 1, por lo cual se considera que carece de nivel inventivo.

Teniendo en cuenta lo señalado en el artículo 18 de la Decisión 486 de 2000 de la Comisión de la Comunidad Andina, la reivindicación independiente 13 (NC2019/0004599 del 24 de mayo de 2022) refiere a: *“Un método para la seguridad del internet de las cosas (IoT, por sus siglas en inglés), que comprende: (...)”*. A continuación, se presenta la tabla comparativa entre el objeto reivindicado y los documentos encontrados en el estado de la técnica:

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

Oficio N° 10562 de 8 de julio de 2022

Ref. Expediente N° NC2019/0004599

CARACTERÍSTICAS ESENCIALES	D1	D2
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).	El método puede incluir además generar un modelo de características para un programa de aplicación específico en la pluralidad de dispositivos (...). (Párr. 0015).
Almacenar (591) un conjunto de reglas de seguridad que están asociadas con una condición esperada de al menos un dispositivo de IoT (341).	(...) 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 análisis incluye una evaluación de reglas. Las reglas pueden ser para eventos específicos o frecuencia de eventos o para eventos o recuento o volumen o solo si son anómalos para el usuario (...). (Párr. 0184).
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).	No se menciona.
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).	No se menciona.
Emplear al menos un procesador para comparar los datos agregados del dispositivo de IoT con el modelo configurable de dispositivo de IoT para determinar 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).	No se menciona.

Oficio N° 10562 de 8 de julio de 2022

Ref. Expediente N° NC2019/0004599

	(...) 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).	
En donde la determinación de si se ha violado el conjunto de reglas de seguridad (593) para el dispositivo IoT, la cual se basa en los datos IoT ya recibidos y ocurre a continuación después de recibir dichos datos IoT.	(...) Reportar la información de comportamiento observada en el dispositivo IoT a una entidad de servicio al cliente en respuesta a la determinación de que la información de comportamiento observada en el dispositivo IoT indica un comportamiento anómalo. (Reiv. 5).	No se menciona.
Depende de otros factores a los utilizados en la determinación de enviar los datos de IoT en respuesta a que se ha excedido el umbral.	No se menciona.	(...) El aumento de la supervisión permite la recopilación de datos adicionales antes de tomar una determinación final sobre la existencia o no de actividad maliciosa (...). (Párr. 0233).
Y 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).	(...) Las respuestas pueden incluir notificaciones y alertas de un usuario, administrador o analista (...). (Párr. 0008).

D1 es considerado como el estado de la técnica más cercano a la invención definida en la reivindicación 13, ya que divulga un método para monitorear el estado del dispositivo de Internet de las cosas (IoT) (...) (Reiv. 1).

La diferencia entre la invención definida entre la reivindicación 13 y el método divulgado en D1, consiste en que la invención incluye la determinación de si se infringió el conjunto de reglas de seguridad para el dispositivo IoT en función de otros factores a los utilizados en la determinación de enviar los datos de IoT en respuesta a que se ha excedido el umbral.

El efecto que se logra al incluir específicamente la determinación de si se infringió el conjunto de reglas de seguridad para el dispositivo IoT en función de otros factores a los utilizados en la determinación de enviar los datos de IoT en respuesta a que se ha excedido el umbral es garantizar un nivel alto de seguridad para los dispositivos IoT de una manera más eficiente.

Por lo tanto, el problema técnico objetivo que pretende resolver esta invención se puede formular así: ¿cómo modificar el método divulgado en D1 para garantizar un nivel alto de seguridad para los dispositivos IoT de una manera más eficiente?.



Oficio N° 10562 de 8 de julio de 2022

Ref. Expediente N° NC2019/0004599

Sin embargo, el incluir la determinación de si se infringió el conjunto de reglas de seguridad para el dispositivo IoT en función de otros factores a los utilizados en la determinación de enviar los datos de IoT en respuesta a que se ha excedido el umbral para garantizar un nivel alto de seguridad para los dispositivos IoT de una manera más eficiente, ya está divulgado en D2 que se refiere a que un mayor monitoreo puede ser apropiado cuando el sistema tiene sospechas de actividad maliciosa, donde el aumento de la supervisión permite la recopilación de datos adicionales antes de tomar una determinación final sobre la existencia o no de actividad maliciosa (Párr. 0233).

En consecuencia, la persona normalmente versada en la materia estaría motivada a incluir la determinación de si se infringió el conjunto de reglas de seguridad para el dispositivo IoT en función de otros factores a los utilizados en la determinación de enviar los datos de IoT en respuesta a que se ha excedido el umbral del D2 en el método de D1, para así llegar al objeto de la reivindicación 13. Por lo cual se considera obvia.

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



Oficio N° 10562 de 8 de julio de 2022

Ref. Expediente N° NC2019/0004599

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 no mencionan alguna característica que, junto con las características de la reivindicación independiente, aporte nivel inventivo al método de la reivindicación 13, por lo cual se considera que carece de nivel inventivo.

Teniendo en cuenta lo señalado en el artículo 18 de la Decisión 486 de 2000 de la Comisión de la Comunidad Andina, la reivindicación independiente 17 (NC2019/0004599 del 24 de mayo de 2022) refiere a: “Un método para la seguridad del internet de las cosas (IoT, por sus siglas en inglés), que comprende: (...)”. A continuación, se presenta la tabla comparativa entre el objeto reivindicado y los documentos encontrados en el estado de la técnica:

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

CARACTERÍSTICAS ESENCIALES	D1	D2
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).	(...) Un contexto describe las condiciones en las que se produce el uso, la falta de uso o ambos del dispositivo. El contexto se puede utilizar para configurar automáticamente el dispositivo informático aplicando las políticas adecuadas. La determinación del contexto permite que el sistema descubra lo que el usuario está haciendo actualmente, anticipe o prediga lo que probablemente hará el usuario a continuación y configure el dispositivo informático en consecuencia. (Párr. 0085).
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).	(...) Un contexto describe las condiciones en las que se produce el uso, la falta de uso o ambos del dispositivo. El contexto se puede utilizar para configurar automáticamente el dispositivo informático aplicando las políticas adecuadas (...). (Párr. 0085). (...) Los datos recopilados comprenden información de contexto asociada con un evento que ocurrió en un dispositivo. (Reiv. 2).
Y 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	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	No se menciona.

Oficio N° 10562 de 8 de julio de 2022

Ref. Expediente N° NC2019/0004599

una combinación de al menos dos tipos diferentes de datos de al menos dos de la pluralidad de dispositivos de IoT considerados en conjunto.	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).	No se menciona.
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).	(...) Las respuestas pueden incluir notificaciones y alertas de un usuario, administrador o analista (...). (Párr. 0008).
En donde la determinación de si se infringió el conjunto ajustado de reglas de seguridad, la cual se basa en los datos IoT ya recibidos y ocurre a continuación después de recibir dichos datos IoT.	(...) Reportar la información de comportamiento observada en el dispositivo IoT a una entidad de servicio al cliente en respuesta a la determinación de que la información de comportamiento observada en el dispositivo IoT indica un comportamiento anómalo. (Reiv. 5).	No se menciona.
Depende de otros factores a los utilizados en la determinación de enviar los datos de IoT en respuesta a que se ha excedido el umbral.	No se menciona.	(...) El aumento de la supervisión permite la recopilación de datos adicionales antes de tomar una determinación final sobre la existencia o no de actividad maliciosa (...). (Párr. 0233).

D1 es considerado como el estado de la técnica más cercano a la invención definida en la reivindicación 17, ya que divulga un método para monitorear el estado del dispositivo de Internet de las cosas (IoT) (...) (Reiv. 1).

La diferencia entre la invención definida entre la reivindicación 17 y el método divulgado en D1, consiste en que la invención incluye la determinación de si se infringió el conjunto de reglas de seguridad para el dispositivo IoT en función de otros factores a los utilizados

Oficio N° **10562** de **8 de julio de 2022**

Ref. Expediente N° NC2019/0004599

en la determinación de enviar los datos de IoT en respuesta a que se ha excedido el umbral.

El efecto que se logra al incluir específicamente la determinación de si se infringió el conjunto de reglas de seguridad para el dispositivo IoT en función de otros factores a los utilizados en la determinación de enviar los datos de IoT en respuesta a que se ha excedido el umbral es garantizar un nivel alto de seguridad para los dispositivos IoT de una manera más eficiente.

Por lo tanto, el problema técnico objetivo que pretende resolver esta invención se puede formular así: ¿cómo modificar el método divulgado en D1 para garantizar un nivel alto de seguridad para los dispositivos IoT de una manera más eficiente?.

Sin embargo, el incluir la determinación de si se infringió el conjunto de reglas de seguridad para el dispositivo IoT en función de otros factores a los utilizados en la determinación de enviar los datos de IoT en respuesta a que se ha excedido el umbral para garantizar un nivel alto de seguridad para los dispositivos IoT de una manera más eficiente, ya está divulgado en D2 que se refiere a que un mayor monitoreo puede ser apropiado cuando el sistema tiene sospechas de actividad maliciosa, donde el aumento de la supervisión permite la recopilación de datos adicionales antes de tomar una determinación final sobre la existencia o no de actividad maliciosa (Párr. 0233).

En consecuencia, la persona normalmente versada en la materia estaría motivada a incluir la determinación de si se infringió el conjunto de reglas de seguridad para el dispositivo IoT en función de otros factores a los utilizados en la determinación de enviar los datos de IoT en respuesta a que se ha excedido el umbral del D2 en el método de D1, para así llegar al objeto de la reivindicación 17. Por lo cual se considera obvia.

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



Oficio N° 10562 de 8 de julio de 2022

Ref. Expediente N° NC2019/0004599

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).

- 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 no mencionan alguna característica que, junto con las características de la reivindicación independiente, aporte nivel inventivo al método de la reivindicación 17, por lo cual se considera que carece de nivel inventivo.

6. Conclusión

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

Ítem	Documento	Reivindicaciones afectadas	Requisito que afecta
D1	WO2016140912	1 a 20	Nivel inventivo
D2	US20150163121	1, 13 y 17	Nivel inventivo

7. Respuesta a los argumentos del solicitante

El solicitante argumenta que “(...) las reivindicaciones 1, 13, y 17 se modificaron con el objetivo de que sea aún más clara su novedad y nivel inventivo donde ahora incluyen que la determinación de si se infringió el conjunto de reglas de seguridad “se basa en los datos IoT ya recibidos y ocurre a continuación después de recibir dichos datos IoT” lo que no está divulgado ni sugerido por los documentos D1 o D2 (...).

(...) La invención del documento D1, cuando transmite los parámetros de comportamiento observados a un servicio al cliente, no realiza la determinación de la violación de las reglas de seguridad a continuación después de su recepción, es decir, no realiza dicha determinación inmediatamente después de su recepción. Por el contrario, el documento D1, en su párrafo [0130] sugiere que, cuando se envían los parámetros de comportamiento observado a un servicio al cliente, para el diagnóstico de un comportamiento anómalo se habilitan mensajes de entrada y salida para recolectar información adicional, lo cual es contrario a lo reclamado en la presente solicitud que determina la violación a las reglas de seguridad con la información ya recibida, sin recolectar información adicional (...)”.

Se aclara que el documento D1 menciona que se reporta la información de comportamiento observada en el dispositivo IoT a una entidad de servicio al cliente en

Oficio N° 10562 de 8 de julio de 2022

Ref. Expediente N° NC2019/0004599

respuesta a la determinación de que la información de comportamiento observada en el dispositivo IoT indica un comportamiento anómalo (Reiv. 5). Por lo tanto, D1 muestra que la transmisión de información recolectada al servicio al cliente para la determinación de la infracción de reglas de seguridad ocurre en respuesta o a continuación de la determinación del comportamiento observado en el dispositivo IoT, de esta manera, este documento si revela que los datos IoT se transmitan inmediatamente o a continuación, para realizar la determinación de anomalías como lo requiere la presente solicitud, afectando así las características reclamadas. Asimismo, es importante aclarar que D2 no menciona la característica referente a que la determinación de la infracción de reglas de seguridad ocurra a continuación de la recepción de los datos IoT.

El solicitante argumenta que “(...) Por su parte, el documento D2 no solventa la mencionada falencia del documento D1 en divulgar la determinación de la violación con información ya recibida e inmediatamente después de recibirla. Por el contrario, el documento D2 requiere de un aumento en la supervisión para recopilación de datos adicionales antes de tomar una determinación final sobre la existencia o no de actividad maliciosa (ver documento D2, párrafo [0233]) (...)”.

En primer lugar, se aclara que no es necesario que el documento D2 revele que la determinación de la infracción de reglas de seguridad ocurra a continuación de la recepción de los datos IoT, ya que dicha característica es anticipada por el documento D1 como se explicó en el argumento anterior. Adicionalmente, se aclara que el documento D2 se utiliza para anticipar la característica referente a la utilización de otros factores o datos adicionales al momento de determinar la infracción de reglas de seguridad, donde dicha característica es anticipada por este documento al afirmar que el aumento de la supervisión permite la recopilación de datos adicionales antes de tomar una determinación final sobre la existencia o no de actividad maliciosa (Párr. 0233). Por lo tanto, teniendo que D2 se encuentra en el mismo campo técnico de la solicitud y resuelve el mismo problema, es posible combinar sus enseñanzas junto a las de D1 para afectar así el carácter inventivo de la característica reclamada.

El solicitante afirma que “(...) Adicionalmente, 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 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.

Estas dos determinaciones permiten que la invención que se reclama garantice un nivel alto de seguridad para los dispositivos IoT de una manera más eficiente (al menos más eficiente que la invención del documento D1), debido a que la primera determinación, que es menos exigente computacionalmente, es la que determina si se envían los datos al concentrador IoT para que, en dicho concentrador, se determine si se infringió el conjunto de reglas de seguridad, lo cual es más exigente computacionalmente que la primera determinación.



Oficio N° 10562 de 8 de julio de 2022

Ref. Expediente N° NC2019/0004599

De acuerdo con lo dicho en el anterior párrafo, la invención que se reclama aumenta la eficiencia porque realiza siempre determinaciones de baja exigencia computacional en el dispositivo IoT y solo realiza envío de datos y posterior procesamiento para determinar una posible violación de seguridad cuando existe un indicio de ello correspondiente a que un valor a excedido un umbral.

En contraste, las invenciones de los documentos D1 y D2 son diferentes y no presentan este efecto mejorado (...)

Con respecto a lo anterior, 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, esta oficina reitera 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.



Oficio N° **10562** de **8 de julio de 2022**

Ref. Expediente N° NC2019/0004599

Adicionalmente, se aclara que la característica de exigencia computacional ofrecida por el aparato y métodos reclamados, no se encuentra divulgada en las reivindicaciones del capítulo estudiado, por lo tanto, no hace parte del estudio de nivel inventivo 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° 10562 de 8 de julio de 2022

Ref. Expediente N° NC2019/0004599

INFORME DE BÚSQUEDA
EXAMEN DE PATENTABILIDAD

Solicitud No.		Examen de patentabilidad							
NC2019/0004599		1°		2°	X	3°		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, Párr. 0121, Párr. 00103, Reiv. 5. 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.				Y	

Oficio N° 10562 de 8 de julio de 2022

Ref. Expediente N° NC2019/0004599

				00129, Párr. 00121, Párr. 00103, Reiv. 5. 14 Párr. 00107, Párr. 00112. 15 Párr. 00101, Párr. 0099. 16 Párr. 00122. 17 Párr. 00143, Párr. 00122, Párr. 00112, Párr. 00109, Párr. 00101, Párr. 00122, Párr. 00113, Párr. 00130, Párr. 00129, Párr. 00103, Reiv. 5. 18 Párr. 00112, Párr. 00107. 19 Párr. 00101, Párr. 0099. 20 Párr. 0046.	
US	US20160212099	21/07/2016	-	-	A
Google Patents	US20150163121	11/06/2015	1, 13 y 17	1 Párr. 0275, Párr. 0276, Párr. 0049, Párr. 0046, Párr. 0015, Párr. 0184, Párr. 0185, Párr. 0008, Párr. 0233. 13 Párr. 0015, Párr. 0184, Párr. 0008, Párr. 0233. 17 Párr. 0085, Reiv. 2, Párr. 0008, Párr. 0233.	Y
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: (05/07/2022)					