Señores
Superintendencia de Industria y Comercio
Dirección de Nuevas Creaciones
E. S. D.

Ref: Expediente No. NC2019/0004599.

Solicitud de registro de Patente de Invención denominada "APARATO Y MÉTODOS PARA SERVICIO DE SEGURIDAD DEL INTERNET DE LAS COSAS".

Entrada en fase nacional de la solicitud PCT/US2017/058926.

Solicitante: MICROSOFT TECHNOLOGY LICENSING, LLC.

Luz Helena Adarve, identificada como aparece al pie de mi firma, y obrando en mi condición de apoderada de **MICROSOFT TECHNOLOGY LICENSING, LLC,** solicitante de la patente en referencia, a continuación, doy respuesta al Oficio **No. 7149** del 18 de junio de 2020.

1. Respecto a la Determinación del Estado de la Técnica y al Examen de Patentabilidad

En los numerales 4, 5 y 6 del oficio citado, ese Despacho concluye que las reivindicaciones de la presente solicitud de patente carecen de novedad frente a las enseñanzas del documento **WO2016140912 (D1).**

1.1. Novedad y Nivel Inventivo

Aunque el Examinador haya citado el documento D1 para objetar la novedad de la presente invención, es posible afirmar que éste no enseña las características esenciales de la invención, como será demostrado a continuación.

Con el fin de superar las objeciones presentadas respecto a la novedad es deseo del solicitante presentar un nuevo capítulo reivindicatorio compuesto por 20 reivindicaciones, que encuentran su debido sustento en las reivindicaciones y la descripción originalmente presentadas, sin que ello conlleve ampliación de la invención.

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

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

El documento D1 se relaciona con el análisis de comportamiento para automatizar el monitoreo del estado del dispositivo de Internet de las cosas (IoT) de manera directa o indirecta. En particular, el comportamiento normal asociado con un dispositivo IoT en una red IoT local puede modelarse de 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 de IoT distribuido, los dispositivos "*analizadores*" más potentes pueden recopilar comportamientos observados localmente en otros dispositivos "*observadores*" (por ejemplo, más simples) y realizar análisis de comportamiento en el entorno de IoT distribuido para detectar anomalías que puedan indicar ataques maliciosos, mal funcionamiento u otros asuntos que requieren servicio al cliente y/o mayor atención. 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.

Por lo tanto, el documento D1 revela la realización de un análisis de comportamiento si los comportamientos observados en un dispositivo IoT son normales o anómalos, ya sea en un dispositivo analizador más potente, que recopila los comportamientos observados localmente en dispositivos IoT más simples, o en dispositivos IoT locales con capacidades suficientes para detectar anomalías. <u>En contraste con esto, la presente solicitud enseña a determinar si se ha violado una regla de seguridad basándose en la detección de una anomalía siempre en un concentrador de IoT</u>. Sin

embargo, la presente solicitud describe además que los dispositivos de IoT "*simples*" están en cualquier caso al menos habilitados para determinar si se ha excedido un umbral basado en uno o más tipos diferentes de datos de IoT para enviar los datos de IoT solo al concentrador de IoT. Por lo tanto, los dispositivos de IoT de la presente solicitud no requieren realizar un análisis de comportamiento completo, pero en cualquier caso pueden determinar si diferentes tipos de datos de IoT están fuera de un umbral particular o no.

La presente solicitud resuelve el problema técnico de garantizar un nivel alto de seguridad para los dispositivos IoT de una manera más eficiente (al menos más eficiente que la invención del documento D1) proporcionando un concentrador IoT, que es capaz de generar un modelo configurable para dispositivos IoT así como almacenar un conjunto de reglas de seguridad asociadas con la condición esperada de al menos un dispositivo IoT. Dicho concentrador de IoT se configura para analizar cualquier dato de IoT recibido de uno o más dispositivos de IoT comparando dichos datos de IoT con el modelo de IoT. Si dicha comparación revela que se ha violado el conjunto de reglas de seguridad, el concentrador de IoT envía una alerta. De esta forma, la presente solicitud garantiza un alto nivel de seguridad en un sistema que comprende una pluralidad de diferentes dispositivos IoT. Además, los propios dispositivos de IoT pueden realizar un análisis básico donde se evalua si un tipo específico de datos de IoT excede un umbral y, por lo tanto, se encuentra fuera de un rango predefinido específico. Solo si dicho primer análisis básico da como resultado algún valor atípico peculiar, los datos de IoT respectivos se envían al concentrador de IoT para realizar un análisis más profundo. Debido a que dicho análisis previo de los datos de IoT se lleva a cabo directamente en los dispositivos de IoT, la cantidad de datos de IoT, que deben transmitirse a través de una red de comunicación al concentrador de IoT, se reduce significativamente. Por lo tanto, la invención de la presente solicitud permite identificar cualquier amenaza de seguridad seguridad para los dispositivos IoT de una manera muy eficiente.

La enseñanza del documento D1 no resuelve el problema de identificación de amenazas de seguridad mencionado de una manera tan eficiente como la presente solicitud. A saber, el documento D1 describe dos casos alternativos (métodos alternativos). El primero donde los dispositivos de IoT transmiten todos los datos de IoT a un potente dispositivo analizador, que posteriormente realiza un análisis de comportamiento para determinar si los comportamientos observados en los dispositivos de IoT son normales o anómalos y, en el segundo caso, los dispositivos IoT están equipados con suficientes capacidades para realizar un análisis de

comportamiento de este tipo para detectar anomalías por sí mismos. Si bien dichos dos métodos alternativos permiten identificar cualquier amenaza para los dispositivos de IoT de forma satisfactoria como en la presente solicitud, ambos métodos alternativos descritos en el documento D1 son, sin embargo, **menos eficientes** computacionalmente que la solución proporcionada en la presente solicitud. Es decir, en la primera alternativa, todos los datos de IoT recopilados en todos los dispositivos de IoT deben transmitirse al dispositivo analizador, lo que da como resultado un mayor tráfico de comunicaciones de red. En la segunda alternativa, por otro lado, todos los dispositivos de IoT deben comprender recursos informáticos avanzados para realizar el análisis de comportamiento completo de los datos de IoT localmente.

Adicionalmente, el solicitante indica que al parecer no hay otros documentos que lleven a la persona del oficio medianamente versada en la materia a concluir la invención de la presente solicitud partiendo del documento D1 o cualquier otro documento. Como evidencia de esto, se indica que las invenciones de documentos US 2015/271033 y US 2015/150124, que corresponden a los documentos citados en el Reporte Preliminar Internacional sobre patentabilidad de la solicitud PCT/US2017/058926, o de los documentos US 2016/0212099 y US 2015/0163121, que fueron citados en la solicitud homologa en los Estados Unidos, no enseñan las características ni información que lleven a la persona del oficio a concluir la invención de la presente solicitud, y, por lo tanto, se concluye que la presente solicitud no solo es novedosa, sino también tiene nivel inventivo.

Por todo lo anterior se concluye que las reivindicaciones de la presente solicitud poseen características que no se dan a conocer de manera obvia para una persona versada en la materia por el documento D1, u otro documento en el estado del arte, por ende, la presente invención debe ser considerada como novedosa y con nivel inventivo sobre el estado de la técnica presentado por el Examinador.

2. Conclusión

Los argumentos expuestos en el numeral 1 del presente escrito ponen de manifiesto de una manera clara y contundente que lo revelado en las nuevas reivindicaciones de la presente solicitud resulta completamente NOVEDOSO E INVENTIVO sobre las enseñanzas del estado del arte más cercano representado por el documento D1, toda vez que nada dentro de dichos documentos revela en forma directa o al menos

llega a sugerir datos de IoT que son recibidos cuando 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 consecuencia, me permito solicitar a ese Despacho, proceder con la revisión de las modificaciones y de los argumentos aquí presentados, para conceder el privilegio de patente solicitado para la materia objeto de las 20 reivindicaciones ahora presentadas en el capítulo reivindicatorio modificado, y que de subsistir alguna duda o inquietud respecto a la patentabilidad de la presente invención, a pesar de las modificaciones y argumentos técnicos ahora presentados, sin apartarse del espíritu inventivo originalmente revelado en la solicitud internacional, se le brinde la oportunidad al solicitante de aclararla o de limitar aún más la invención, mediante la emisión de un segundo examen de fondo, teniendo en cuenta el nuevo capítulo reivindicatorio que se somete a revisión, antes de que se emita una decisión definitiva por parte de ese Despacho, de conformidad con lo dispuesto en 1.2.2.5.1 del artículo primero de la Resolución 54093 de 2012.

3. Anexos

Junto con este escrito se incluye lo siguiente:

- Capítulo reivindicatorio modificado, en donde se han llevado a cabo las modificaciones mencionadas anteriormente.

4. Pagos

Junto con esta respuesta se paga la tasa correspondiente a la modificación del capítulo reivindicatorio.

Petición

Solicito al Despacho, y en el evento que el examinador considere que pese a las modificaciones presentadas aún existen objeciones, que proceda a emitir un segundo examen de fondo sobre el nuevo capítulo reivindicatorio presentado.

En este sentido requiero se me comunique a través del SIPI o cualquier otro medio la existencia de estas objeciones para, de esta manera, si procede, realizar el nuevo pago del examen de patentabilidad de la solicitud de la referencia.

Atentamente,

LUZ HELENA ADARVE GÓMEZ.
C.C 41.575.435 de Bogotá.
T.P. 14.884 C.S.J.

_____

FJG
P-1059

REIVINDICACIONES (con marcas de modificación)

1. Un aparato para la seguridad del internet de las cosas (IoT, por sus siglas en inglés), que comprende:

un concentrador de IoT que incluye uno o más dispositivos, los dispositivos incluyen al menos una memoria adaptada para almacenar los datos en tiempo de ejecución para los dispositivos, 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 realice las acciones, que incluyen:

generar un modelo configurable de dispositivo de IoT;

almacenar un conjunto de reglas de seguridad que están asociadas con una condición esperada de al menos un dispositivo de IoT, el conjunto de reglas de seguridad estando basado en información de operación recibida de cada uno de una pluralidad de dispositivos de IoT;

recibir datos de IoT asociados con al menos un dispositivo de IoT cuando dicho al menos un dispositivo de IoT determina enviar los datos de IoT en respuesta a que se ha excedido un umbral basado en uno o más de los tipos de datos, en donde los datos de IoT son datos agregados que incluyen al menos dos tipos diferentes de datos;

determinar, para cada dispositivo de IoT del al menos un dispositivo IoT, con base en los datos de IoT y en el modelo de dispositivo de IoT, si se infringió el conjunto de reglas de seguridad para el dispositivo IoT con base en información de operación recibida de cada uno de una pluralidad de dispositivos de IoT de tal manera que la determinación está basada en una combinación de al menos dos tipos diferentes de datos de al menos dos de la pluralidad de dispositivos de IoT considerados en conjunto; y

enviar selectivamente una alerta con base en la determinación.

2. El aparato de acuerdo con la reivindicación 1, en donde las acciones incluyen, además:

recibir una solicitud de configuración; y

ajustar el conjunto de reglas de seguridad con base en la solicitud de configuración.

3. El aparato de acuerdo con la reivindicación 1, en donde los datos de IoT se recibe de un agente de recopilación de datos implementado en el al menos un dispositivo de IoT.

4. El aparato de acuerdo con la reivindicación 1, en donde el al menos un dispositivo de IoT incluye una pluralidad de dispositivos de IoT, y en donde los datos de IoT se reciben de parte de los agentes de recopilación de datos implementados en la pluralidad de dispositivos de IoT.

5. El aparato de acuerdo con la reivindicación 1, en donde el conjunto de reglas de

seguridad incluye al menos una lista blanca de procesoso una lista negra de procesos.

6. El aparato de acuerdo con la reivindicación 1, en donde los datos de IoT incluyen un estado de un interruptor de manipulación en al menos un dispositivo de IoT.

7. El aparato de acuerdo con la reivindicación 1, en donde los datos de IoT se agregan desde múltiples dispositivos de IoT que incluyen al menos un dispositivo de IoT.

8. El aparato de acuerdo con la reivindicación 1, en donde los datos agregados de los datos de IoT incluyen datos de entorno y datos de estado interno.

9. El aparato de acuerdo con la reivindicación 8, en donde los datos de entorno incluyen al menos una de temperatura, humedad, ubicación detectada o geolocalización

10. El aparato de acuerdo con la reivindicación 8, en donde los datos internos incluyen al menos uno de una versión del sistema operativo, estado actual de procesos activos, puertos abiertos o información asociada con dispositivos conectados a el al menos un dispositivo de IoT.

11. El aparato de acuerdo con la reivindicación 1, en donde el conjunto de reglas de seguridad son de tal manera que la infracción del conjunto de reglas de seguridad indica al menos una posibilidad de un ataque, en donde el ataque es al menos uno de un ataque físico o un ciberataque en el al menos un dispositivo de IoT.

12. El aparato de acuerdo con la reivindicación 1, en donde enviar selectivamente una alerta con base en la determinación además incluye enviar selectivamente información sobre el ataque con la alerta.

13. Un método para la seguridad del internet de las cosas (IoT, por sus siglas en inglés), que comprende:

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;

almacenar un conjunto de reglas de seguridad que están asociadas con una condición esperada de al menos un dispositivo de IoT;

recibir los datos agregados del dispositivo de IoT desde al menos un dispositivo de IoT cuando dicho al menos un dispositivo de IoT determina enviar los datos de IoT en respuesta a que se ha excedido un umbral basado en uno o más de los tipos de datos, en donde los datos agregados del dispositivo de IoT incluyen al menos dos tipos diferentes de datos de la pluralidad de dispositivos de IoT;

emplear al menos un procesador para comparar los datos agregados del dispositivo de IoT

con el modelo configurable de dispositivo de IoT en cuanto a si se ha violado el conjunto de reglas de seguridad de tal manera que la comparación se evalua con base en una combinación de al menos dos tipos diferentes de datos de al menos dos de la pluralidad de dispositivos de IoT considerados en conjunto; y

enviar selectivamente una alerta con base en la comparación.

14. El método de acuerdo con la reivindicación 13, en donde al menos un dispositivo de IoT incluye una pluralidad de dispositivos de IoT, y en donde los datos agregados del dispositivo de IoT se reciben de parte de los agentes de recopilación de datos implementados en la pluralidad de dispositivos de IoT.

15. El método de acuerdo con la reivindicación 13, en donde los datos agregados de los datos de dispositivo IoT incluyen datos de entorno y datos de estado interno.

16. El método de acuerdo con la reivindicación 13, que comprende, además:

recibir una solicitud de configuración; y

ajustar el modelo configurable de dispositivo de IoT con base en la solicitud de configuración.

17. Un método para la seguridad del internet de las cosas (IoT, por sus siglas en inglés), que comprende:

emplear al menos un procesador para generar una solicitud de configuración, en donde la solicitud de configuración es una solicitud para cambiar un conjunto de reglas de seguridad a un conjunto ajustado de reglas de seguridad, en donde el conjunto ajustado de reglas de seguridad está asociado con una condición esperada de al menos un dispositivo de IoT, 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, y en donde los datos de IoT son datos agregados que son recibidos de al menos un dispositivo de IoT cuando dicho al menos un dispositivo de IoT determina enviar los datos de IoT en respuesta a que se ha excedido un umbral basado en uno o más de los tipos de datos y que incluyen al menos dos tipos diferentes de datos de la pluralidad de dispositivos de IoT de manera que la aplicación del conjunto ajustado de reglas de seguridad está basado en una combinación de al menos dos tipos diferentes de datos de al menos dos de la pluralidad de dispositivos de IoT considerados en conjunto;

enviar la solicitud de configuración a un concentrador de IoT; y

recibir una alerta del concentrador de IoT cuando el concentrador de IoT determina que se infringió el conjunto ajustado de reglas de seguridad.

18. El método de acuerdo con la reivindicación 17, en donde el conjunto ajustado de reglas de seguridad se basa en una evaluación de los datos de IoT asociados con al menos un

dispositivo de IoT de tal manera que al menos un dispositivo de IoT sea una pluralidad de dispositivos de IoT.

19. El método de acuerdo con la reivindicación 17, en donde los datos agregados de los datos de IoT incluyen los datos de entorno y los datos internos.

20. El método de acuerdo con la reivindicación 19, donde los datos de entorno incluyen al menos una de temperatura, humedad, ubicación detectada o geolocalización, y donde los datos internos incluyen al menos uno de la versión del sistema operativo, estado actual de procesos activos, puertos abiertos, o información asociada con los dispositivos conectados a al menos un dispositivo de IoT.

REIVINDICACIONES

1. Un aparato para la seguridad del internet de las cosas (IoT, por sus siglas en inglés), que comprende:

un concentrador de IoT que incluye uno o más dispositivos, los dispositivos incluyen al menos una memoria adaptada para almacenar los datos en tiempo de ejecución para los dispositivos, 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 realice las acciones, que incluyen:

generar un modelo configurable de dispositivo de IoT;

almacenar un conjunto de reglas de seguridad que están asociadas con una condición esperada de al menos un dispositivo de IoT, el conjunto de reglas de seguridad estando basado en información de operación recibida de cada uno de una pluralidad de dispositivos de IoT;

recibir datos de IoT asociados con al menos un dispositivo de IoT cuando dicho al menos un dispositivo de IoT determina enviar los datos de IoT en respuesta a que se ha excedido un umbral basado en uno o más de los tipos de datos, en donde los datos de IoT son datos agregados que incluyen al menos dos tipos diferentes de datos;

determinar, para cada dispositivo de IoT del al menos un dispositivo IoT, con base en los datos de IoT y en el modelo de dispositivo de IoT, si se infringió el conjunto de reglas de seguridad para el dispositivo IoT con base en información de operación recibida de cada uno de una pluralidad de dispositivos de IoT de tal manera que la determinación está basada en una combinación de al menos dos tipos diferentes de datos de al menos dos de la pluralidad de dispositivos de IoT considerados en conjunto; y

enviar selectivamente una alerta con base en la determinación.

2. El aparato de acuerdo con la reivindicación 1, en donde las acciones incluyen, además:

recibir una solicitud de configuración; y

ajustar el conjunto de reglas de seguridad con base en la solicitud de configuración.

3. El aparato de acuerdo con la reivindicación 1, en donde los datos de IoT se recibe de un agente de recopilación de datos implementado en el al menos un dispositivo de IoT.

4. El aparato de acuerdo con la reivindicación 1, en donde el al menos un dispositivo de IoT incluye una pluralidad de dispositivos de IoT, y en donde los datos de IoT se reciben de parte de los agentes de recopilación de datos implementados en la pluralidad de dispositivos de IoT.

5. El aparato de acuerdo con la reivindicación 1, en donde el conjunto de reglas de

seguridad incluye al menos una lista blanca de procesoso una lista negra de procesos.

6. El aparato de acuerdo con la reivindicación 1, en donde los datos de IoT incluyen un estado de un interruptor de manipulación en al menos un dispositivo de IoT.

7. El aparato de acuerdo con la reivindicación 1, en donde los datos de IoT se agregan desde múltiples dispositivos de IoT que incluyen al menos un dispositivo de IoT.

8. El aparato de acuerdo con la reivindicación 1, en donde los datos agregados de los datos de IoT incluyen datos de entorno y datos de estado interno.

9. El aparato de acuerdo con la reivindicación 8, en donde los datos de entorno incluyen al menos una de temperatura, humedad, ubicación detectada o geolocalización

10. El aparato de acuerdo con la reivindicación 8, en donde los datos internos incluyen al menos uno de una versión del sistema operativo, estado actual de procesos activos, puertos abiertos o información asociada con dispositivos conectados a el al menos un dispositivo de IoT.

11. El aparato de acuerdo con la reivindicación 1, en donde el conjunto de reglas de seguridad son de tal manera que la infracción del conjunto de reglas de seguridad indica al menos una posibilidad de un ataque, en donde el ataque es al menos uno de un ataque físico o un ciberataque en el al menos un dispositivo de IoT.

12. El aparato de acuerdo con la reivindicación 1, en donde enviar selectivamente una alerta con base en la determinación además incluye enviar selectivamente información sobre el ataque con la alerta.

13. Un método para la seguridad del internet de las cosas (IoT, por sus siglas en inglés), que comprende:

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;

almacenar un conjunto de reglas de seguridad que están asociadas con una condición esperada de al menos un dispositivo de IoT;

recibir los datos agregados del dispositivo de IoT desde al menos un dispositivo de IoT cuando dicho al menos un dispositivo de IoT determina enviar los datos de IoT en respuesta a que se ha excedido un umbral basado en uno o más de los tipos de datos, en donde los datos agregados del dispositivo de IoT incluyen al menos dos tipos diferentes de datos de la pluralidad de dispositivos de IoT;

emplear al menos un procesador para comparar los datos agregados del dispositivo de IoT

con el modelo configurable de dispositivo de IoT en cuanto a si se ha violado el conjunto de reglas de seguridad de tal manera que la comparación se evalua con base en una combinación de al menos dos tipos diferentes de datos de al menos dos de la pluralidad de dispositivos de IoT considerados en conjunto; y

enviar selectivamente una alerta con base en la comparación.

14. El método de acuerdo con la reivindicación 13, en donde al menos un dispositivo de IoT incluye una pluralidad de dispositivos de IoT, y en donde los datos agregados del dispositivo de IoT se reciben de parte de los agentes de recopilación de datos implementados en la pluralidad de dispositivos de IoT.

15. El método de acuerdo con la reivindicación 13, en donde los datos agregados de los datos de dispositivo IoT incluyen datos de entorno y datos de estado interno.

16. El método de acuerdo con la reivindicación 13, que comprende, además:

recibir una solicitud de configuración; y

ajustar el modelo configurable de dispositivo de IoT con base en la solicitud de configuración.

17. Un método para la seguridad del internet de las cosas (IoT, por sus siglas en inglés), que comprende:

emplear al menos un procesador para generar una solicitud de configuración, en donde la solicitud de configuración es una solicitud para cambiar un conjunto de reglas de seguridad a un conjunto ajustado de reglas de seguridad, en donde el conjunto ajustado de reglas de seguridad está asociado con una condición esperada de al menos un dispositivo de IoT, 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, y en donde los datos de IoT son datos agregados que son recibidos de al menos un dispositivo de IoT cuando dicho al menos un dispositivo de IoT determina enviar los datos de IoT en respuesta a que se ha excedido un umbral basado en uno o más de los tipos de datos y que incluyen al menos dos tipos diferentes de datos de la pluralidad de dispositivos de IoT de manera que la aplicación del conjunto ajustado de reglas de seguridad está basado en una combinación de al menos dos tipos diferentes de datos de al menos dos de la pluralidad de dispositivos de IoT considerados en conjunto;

enviar la solicitud de configuración a un concentrador de IoT; y

recibir una alerta del concentrador de IoT cuando el concentrador de IoT determina que se infringió el conjunto ajustado de reglas de seguridad.

18. El método de acuerdo con la reivindicación 17, en donde el conjunto ajustado de reglas de seguridad se basa en una evaluación de los datos de IoT asociados con al menos un

dispositivo de IoT de tal manera que al menos un dispositivo de IoT sea una pluralidad de dispositivos de IoT.

19. El método de acuerdo con la reivindicación 17, en donde los datos agregados de los datos de IoT incluyen los datos de entorno y los datos internos.

20. El método de acuerdo con la reivindicación 19, donde los datos de entorno incluyen al menos una de temperatura, humedad, ubicación detectada o geolocalización, y donde los datos internos incluyen al menos uno de la versión del sistema operativo, estado actual de procesos activos, puertos abiertos, o información asociada con los dispositivos conectados a al menos un dispositivo de IoT.