

REPÚBLICA DE COLOMBIA
SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO

Oficio N° 3039 de 25 de febrero de 2026

Ref. Expediente N° NC2022/0012870

Señores

CORPORACIÓN UNIVERSITARIA MINUTO DE DIOS - UNIMINUTO

TÍTULO DE LA SOLICITUD: “SISTEMA DE DETECCIÓN TEMPRANA DE INUNDACIÓN”

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 27 de octubre de 2025 bajo el número NC2025/0014969, 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 contar con un sistema autónomo, eficiente y de bajo consumo energético que permita detectar de manera temprana posibles eventos de inundación, especialmente en zonas vulnerables o de difícil acceso, mediante la recolección, transmisión y análisis de datos ambientales en tiempo real.

Para resolver dicho problema técnico, la solicitud en estudio plantea un sistema distribuido compuesto por nodos sensores autónomos y un gateway central, que se comunican mediante tecnología LoRa de bajo consumo energético. Cada nodo incorpora un procesador con capacidad de gestión energética a través de paneles solares y módulos de carga USB, además de interfaces de expansión y mantenimiento.

3. Reivindicaciones estudiadas

El presente estudio se basa en el capítulo reivindicatorio presentado el 27 de octubre de 2025

4. Determinación del Estado de la Técnica

La fecha para determinar el estado de la técnica es el 09 de septiembre de 2022, que corresponde a la fecha de presentación.

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

Oficio N° 3039 de 25 de febrero de 2026

Ref. Expediente N° NC2022/0012870

Ítem	Documento	Título	Fecha de publicación
D1	US2010156632	"Infrastructure monitoring system and method"	24 de junio de 2010
D3	US2019226898	"Environmental sensor platform, system and method"	25 de julio de 2019

D1¹ divulga un sistema y método de monitoreo de infraestructura que comprende múltiples dispositivos de monitoreo y/o múltiples dispositivos de salida. Cada dispositivo de monitoreo incluye al menos un sensor para recopilar datos, un dispositivo de almacenamiento para almacenarlos, un procesador para analizarlos y un dispositivo de comunicaciones para transmitirlos y recibirlos. (...) (Resumen).

D3² divulga un sistema, un método y un medio legible por computadora, configurados para monitorear la altura del nivel del agua en una o más masas de agua. En una versión, el sistema generalmente comprende uno o más de los siguientes componentes: (a) una pluralidad de nodos sensores, cada uno asociado a una ubicación geográfica predeterminada cerca del agua, donde cada nodo sensor comprende: (i) un detector configurado para recopilar datos ambientales sobre los cambios en la altura de la superficie del agua; (...) (Resumen).

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 (NC2025/0014969 del 27 de octubre de 2025) refiere a: *"Sistema de detección temprana de inundación, que comprende: un primer procesador (45) conectado a una interfaz de radio (49) (...)".* A continuación, se presenta la tabla comparativa entre el objeto reivindicado y los documentos encontrados en el estado de la técnica:

CARACTERÍSTICAS ESENCIALES	D1	D3
Sistema de detección temprana de inundación, que comprende:	(...) un sistema (100) de la invención para monitorear, controlar y comunicarse con al menos un dispositivo de monitoreo y/o al menos un dispositivo de control. (Párr. 0029)	(...) se incluyen plataformas, sistemas, métodos y medios informáticos configurados para monitorear los niveles de agua en un área metropolitana u otra área geográfica ubicada cerca de uno o más cuerpos de agua u otras áreas superficiales propensas a inundaciones. (Párr. 0042)
Un primer procesador (45) conectado a una interfaz de radio (49).	(...) un procesador y una memoria contenidos en la carcasa para operar el al menos un transceptor y el al menos un sensor magnético para medir la	En ciertas versiones, el dispositivo de enlace (302) de la computadora (310) está configurado para proporcionar potencia de procesamiento que gestiona múltiples canales de

¹<http://patents.google.com/patent/US20100156632A1/en?q=US2010156632>

²<http://patents.google.com/patent/US20190226898A1/en?q=US2019226898>



Oficio N° 3039 de 25 de febrero de 2026

Ref. Expediente N° NC2022/0012870

	característica magnética medible, (...) (Párr. 0037) La comunicación puede ocurrir a través de cualquier red de comunicaciones (115) conocida en la técnica, incluyendo, pero no limitado a, redes cableadas, redes inalámbricas, redes Zigbee, redes Bluetooth, redes Z-wave, redes WiFi, redes WiMax, redes RF, redes de área local (LAN), redes de Internet, redes de área amplia (WAN), red de telefonía celular, redes telefónicas cableadas, redes inalámbricas de 900 MHz y redes satelitales. (Párr. 0029)	comunicación entre uno o más nodos de sensores (200) y la plataforma en la nube (400). (Párr. 0072)
Una interfaz de mantenimiento (51).	Se ha descubierto sorprendentemente que los dispositivos de monitoreo con capacidades de comunicación unidireccional o bidireccional se pueden usar para detectar fallas en los sistemas del municipio y brindar información sobre el estado, el mantenimiento y el control de los sistemas en tiempo real o casi real, a pedido. (Párr. 0026)	La transmisión de datos a intervalos periódicos también funciona como un "ping" o "latido" que indica que el nodo sensor (200) sigue funcionando y en comunicación con la plataforma en la nube (400). Este enfoque permite supervisar el estado del nodo sensor (200), garantizando su correcto funcionamiento. Por ejemplo, si transcurre un tiempo prolongado desde la última transmisión de datos, como tres veces la frecuencia del intervalo periódico, la plataforma en la nube (400) puede configurarse para determinar que el nodo sensor (200) ha fallado o ha perdido la comunicación. (Párr. 0059)
Y una interfaz electrónica de expansión (47) adaptada por sus periféricos a unos sensores (48).	La unidad de dispositivo de monitoreo (200) incluye un procesador (205). El procesador (205) está acoplado a al menos un puerto de entrada (210) para recibir datos de los sensores (215). (Párr. 0037)	En algunas versiones, los nodos sensores (200) pueden estar equipados con uno o más detectores sensores ambientales variables (202) para recopilar datos ambientales (...) (Párr. 0051)
Un circuito integrado de identificación (46) conectado al primer procesador (45).	El procesador (205) compila al menos una parte de los datos almacenados en la unidad de almacenamiento de datos (230) para transmitirlos al centro de operaciones. (Párr. 0037)	No menciona
Y un subsistema de gestión de energía (43) para cargar la batería de energía interna (44).	En las realizaciones preferidas, el procesador (205) está conectado a una fuente de alimentación (235). Esta fuente puede ser un dispositivo capaz de alimentar el procesador (205) y los dispositivos conectados a él.	Preferiblemente, para soportar el nodo sensor (200) de manera autónoma, este utilizará un cargador de batería (232) conectado operativamente a un módulo fotovoltaico, también conocido como panel solar (234). Preferiblemente, el panel solar



Oficio N° 3039 de 25 de febrero de 2026

Ref. Expediente N° NC2022/0012870

	(Párr. 0038) El procesador (305) está acoplado a una fuente de alimentación (335). La fuente de alimentación (335) puede ser cualquier dispositivo capaz de alimentar el procesador (305) y cualquier dispositivo conectado al procesador (305). (Párr. 0059) Para un técnico medianamente versado en la materia, resulta evidente que se describen los elementos que hacen necesaria y viable la gestión de energía encargada de la carga de la batería, a saber: la batería como fuente de alimentación, la incorporación de fuentes renovables que implican procesos de recarga, y la implementación de una lógica de ahorro energético orientada a optimizar el consumo.	(234) se monta en el exterior del sensor del nodo (200) y funcionará para proporcionar electricidad solar a las baterías (230) a través del cargador de batería (232) a lo largo del tiempo. (Párr. 0061)
Y un segundo procesador (55) que tiene conectada una interfaz de radio LoRa (58).	No menciona	De manera similar, el sensor del módulo de telemetría (204) puede transmitir los datos ambientales al dispositivo de enlace (302) o a la plataforma basada en la nube (400) a través de varias formas de infraestructura de protocolo de comunicación inalámbrica (317), como la transmisión de mensajes a través de un punto de acceso Wi-Fi local, a través de una red de área amplia de baja potencia (LPWAN) como LoRa/LoRaWAN, a través de un operador celular o un servicio general de radio por paquetes (GPRS) (...) (Párr. 0056)
Y módulos de comunicación Wifi (56) y/o GSM (57).	La comunicación puede ocurrir a través de cualquier red de comunicaciones (115) conocida en la técnica, incluidas, entre otras, redes cableadas, redes inalámbricas, redes Zigbee, redes Bluetooth, redes Z-wave, redes WiFi, (...) (Párr. 0029) (...) red de telefonía celular (...) (Párr. 0029)	(...) a través de un operador celular o un servicio general de radio por paquetes (GPRS) (...) (Párr. 0056)
A través de dichos módulos, el segundo procesador (55) se conecta un servidor (59) que administra una base de datos (60).	En dichas implementaciones, el centro de operaciones (105) puede aprovechar la computación en la nube (por ejemplo, una red de computadoras, servidores y	(...) la plataforma en la nube que comprende uno o más servidores en la nube que comprenden un procesador de servidor en la nube y medios de almacenamiento legibles por computadora no transitorios



Oficio N° 3039 de 25 de febrero de 2026

Ref. Expediente N° NC2022/0012870

	dispositivos de almacenamiento de datos alojados remotamente). (Párr. 0036)	codificados con un programa de computadora que incluye instrucciones ejecutables por el procesador de servidor en la nube para crear una aplicación de plataforma en la nube que comprende (...) (Reiv. 1) ii) un módulo de software configurado para aplicar un algoritmo a los datos ambientales para determinar una tendencia o condición ambiental; (Reiv. 1)
Y una interfaz de mantenimiento (54); en donde el segundo procesador (55) está configurado para iniciar sesión en el servidor (59).	Una red de dispositivos de monitorización de la invención es capaz de proporcionar a un administrador del sistema una imagen completa del estado actual del sistema. (Párr. 0027)	Antes de importar un mensaje, la fuente de datos externa debe autenticarse en la plataforma en la nube (400). El ingestor gestiona el proceso de autenticación. Las fuentes de datos externas envían datos de autenticación al ingestor. Estos datos se presentan en forma de nombre de usuario y contraseña o una clave de autenticación. El ingestor recibe los datos de autenticación y los transmite al servicio de seguridad (426) para su autenticación. Este servicio compara los datos de autenticación con los del dispositivo almacenados en el servicio de almacenamiento (414). Si ambas fuentes de datos coinciden, el servicio de seguridad aprueba la solicitud de acceso de las fuentes de datos externas. (Párr. 0088)
Cargar la lista del número de identificación de las tarjetas electrónicas autorizadas;	En las implementaciones preferidas, a cada dispositivo de monitoreo (110) y a cada dispositivo de control (111) se le asigna un identificador único. Este identificador único puede estar relacionado con la ubicación geográfica, la dirección, el orden de instalación o cualquier otro método de identificación. Además, los diferentes tipos de dispositivos (110) y (111) pueden tener identificadores únicos. Por ejemplo, el identificador de todos los medidores de agua puede comenzar con WM, mientras que el de todos los detectores de fugas puede comenzar con LD. Cada comunicación entre los dispositivos (110) y (111) puede incluir el identificador único para que el mensaje sea recibido por el dispositivo (110) o (111) correcto, o el centro de	En general, la plataforma basada en la nube (400) utiliza múltiples servicios para proporcionar administración de dispositivos, ingesta, transformación, análisis, almacenamiento y visualización de los datos ambientales recopilados por la pluralidad de nodos de sensores (200). Preferiblemente, como se ilustra en la FIG. 6, una realización de la plataforma en la nube comprende un servicio de administración de dispositivos (402), (...) (Párr. 0080)



Oficio N° 3039 de 25 de febrero de 2026

Ref. Expediente N° NC2022/0012870

	operaciones (105) pueda determinar desde dónde se envió el mensaje. (Párr. 0032)	
Recibir las tramas de los nodos sensores a través de LoRa (58), (...)	No se menciona	El módulo de telemetría de entrada (304) está configurado para recibir datos del módulo de telemetría del sensor (206). En ciertas versiones, el módulo de telemetría de entrada (304) es utilizado por el dispositivo de enlace (302) para recibir de forma inalámbrica datos ambientales de varios nodos sensores (200). En una versión, el módulo de telemetría de entrada (304) incluye un receptor/concentrador LoRa configurado para proporcionar un enlace de comunicación hacia y desde los nodos sensores (200). (Párr. 0071)
Separar los campos de la información de la trama recibida y comparar el número de identificación de la tarjeta electrónica con la lista; (...)	En las implementaciones preferidas, a cada dispositivo de monitoreo (110) y a cada dispositivo de control (111) se le asigna un identificador único. Este identificador único puede estar relacionado con la ubicación geográfica, la dirección, el orden de instalación o cualquier otro método de identificación. Además, los diferentes tipos de dispositivos (110) y (111) pueden tener identificadores exclusivos para cada tipo de dispositivo. (Párr. 0029)	Antes de importar un mensaje, la fuente de datos externa debe autenticarse en la plataforma en la nube (400). El ingestor gestiona el proceso de autenticación. Las fuentes de datos externas envían datos de autenticación al ingestor. Estos datos se presentan en forma de nombre de usuario y contraseña o una clave de autenticación. El ingestor recibe los datos de autenticación y los transmite al servicio de seguridad (426) para su autenticación. El servicio de seguridad (426) compara los datos de autenticación con los datos de autenticación del dispositivo almacenados en el servicio de almacenamiento (414). (Párr. 0088)
Preguntar si el número de identificación es válido y, cuando es válido, formatear los campos de la información.	(...) a cada dispositivo de monitoreo (110) y a cada dispositivo de control (111) se le asigna un identificador único. Este identificador único puede estar relacionado con la ubicación geográfica, la dirección, el orden de instalación o cualquier otro método de identificación. Además, los diferentes tipos de dispositivos (110) y (111) pueden tener identificadores únicos. Por ejemplo, el identificador de todos los medidores de agua puede comenzar con un WM, mientras que el identificador de todos los detectores de fugas puede	En una versión, un servicio de procesamiento de flujo (412) está configurado para normalizar los datos ambientales recibidos de cada sensor, comprendiendo la normalización la eliminación de datos erróneos, la eliminación de datos atípicos, el marcado de datos erróneos, la interpolación de datos faltantes y el marcado de datos atípicos. (Párr. 0094) Plataforma según la reivindicación 1, en la que al menos un nodo sensor comprende además: un módulo de recopilación de datos,



	comenzar con un LD. Cada comunicación hacia y desde un dispositivo (110) y (111) puede incluir el identificador único para que el mensaje sea recibido por el dispositivo (110) o (111) correcto, o el centro de operaciones (105) pueda determinar desde dónde se envió el mensaje. (Párr. 0032)	comprendiendo el módulo de recopilación de datos un procesador y un medio de almacenamiento legible por computadora no transitorio codificado con un programa de computadora que incluye instrucciones ejecutables por el procesador para crear una aplicación de módulo de recopilación de datos que comprende: un módulo de software configurado para recibir y formatear los datos ambientales en un mensaje configurado operativamente para su transmisión; y un módulo de software configurado para transmitir de forma inalámbrica los datos ambientales a través del módulo de telemetría. (Reiv. 4)
Y enviar la información a la base de datos (60), y cuando no es válido, rechazar la trama y bloquear el dispositivo que intenta acceder al gateway.	El procesador (205) también está conectado a un transceptor (220) para enviar y recibir señales. En las implementaciones preferidas, el procesador (205) está conectado a una unidad de almacenamiento de datos (230). Esta unidad puede almacenar una cantidad predeterminada de datos recibidos de los sensores (215). Por ejemplo, puede almacenar datos durante un tiempo predeterminado (por ejemplo, un día, una semana o un mes), un número predeterminado de lecturas (por ejemplo, 10, 100 o 1000 lecturas) o hasta que el centro de operaciones indique su eliminación. (Párr. 0037) Preferiblemente, la comunicación se realiza mediante un componente inalámbrico, por ejemplo, desde el dispositivo de monitoreo remoto o el dispositivo de control a una instalación de monitoreo regional o a monitores distribuidos. También es preferible que las comunicaciones estén protegidas o cifradas, de modo que el sistema de comunicaciones no pueda ser monitoreado por terceros desconocidos. El acceso al sistema se otorga preferiblemente mediante nombres de usuario y contraseñas, aunque se pueden	Como se ilustra en la FIG. 9, en ciertas versiones, la plataforma en la nube (400) puede comprender un servicio de almacenamiento (414) que está configurado para almacenar mensajes y datos de soporte en uno o más medios de almacenamiento legibles por computadora (408) recibidos por el servicio de ingestión (410) y procesados por el servicio de procesamiento de flujo (412). (Párr. 0114) Para los nodos de sensor (200) y las puertas de enlace (302) que se conectan directamente a la plataforma en la nube (400), el servicio de ingesta (410) utiliza el servicio de seguridad (426) para autenticar los dispositivos. Estos dispositivos deben autenticarse antes de la transmisión de datos. Si no se concede la autorización, el servicio de ingesta (410) rechazará cualquier mensaje entrante del dispositivo no autorizado. (Párr. 0136)



Oficio N° 3039 de 25 de febrero de 2026

Ref. Expediente N° NC2022/0012870

	emplear métodos de cifrado adicionales o alternativos. (Párr. 0027)	
--	--	--

D1 es considerado como el estado de la técnica más cercano a la invención definida en la reivindicación 1, ya que divulga un sistema y método de monitoreo de infraestructura que comprende múltiples dispositivos de monitoreo y/o múltiples dispositivos de salida. Cada dispositivo de monitoreo incluye al menos un sensor para recopilar datos, un dispositivo de almacenamiento para almacenarlos, un procesador para analizarlos y un dispositivo de comunicaciones para transmitirlos y recibirlos. (...) (Resumen).

La diferencia entre la invención definida entre la reivindicación 1 y el método y sistema divulgado en D1, consiste en un segundo procesador que tiene conectada una interfaz de radio LoRa.

El efecto que se logra al incluir específicamente consiste en un segundo procesador que tiene conectada una interfaz de radio LoRa es que la interfaz de radio se enlaza inalámbricamente a través de la interfaz LoRa, comunicando la información generada por el procesador principal al procesador secundario.

Por lo tanto, el problema técnico objetivo que pretende resolver esta invención se puede formular así: ¿cómo modificar método y sistema divulgado en D1 para proporcionar la interfaz de radio que se enlace inalámbricamente a través de la interfaz LoRa, comunicando la información generada por el procesador?

Sin embargo, el incluir un segundo procesador que tiene conectada una interfaz de radio LoRa para que la interfaz de radio se enlace inalámbricamente a través de la interfaz LoRa comunicando la información generada por el procesador principal al procesador secundario ya está divulgado en D3 que se refiere a que de manera similar, el sensor de El módulo de telemetría (204) puede transmitir los datos ambientales al dispositivo de enlace (302) o a la plataforma basada en la nube (400) a través de varias formas de infraestructura de protocolo de comunicación inalámbrica (317), como la transmisión de mensajes a través de un punto de acceso Wi-Fi local, a través de una red de área amplia de baja potencia (LPWAN) como LoRa/LoRaWAN, a través de un operador celular o un servicio general de radio por paquetes (GPRS) (...) (Párr. 0056)

En consecuencia, la persona normalmente versada en la materia estaría motivada a incluir un segundo procesador que tiene conectada una interfaz de radio LoRa del D3 en el sistema 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: La figura 2 muestra un esquema de una unidad de dispositivo de monitoreo (200). Esta unidad incluye un procesador (205). El procesador (205) está conectado a al menos un puerto de entrada (210) para recibir datos de los sensores (215). También está conectado a un transceptor (220) para enviar y recibir señales. En las implementaciones preferidas, el procesador (205) está conectado a una unidad de almacenamiento de datos (230). Esta unidad puede almacenar una cantidad predeterminada de datos recibidos de los sensores (215). Por ejemplo, puede almacenar datos durante un tiempo predeterminado (por ejemplo, un día, una semana o un mes), un número predeterminado de lecturas (por ejemplo, 10, 100 o 1000 lecturas) o hasta que el centro de operaciones indique su eliminación. (Párr. 0037).

Oficio N° 3039 de 25 de febrero de 2026

Ref. Expediente N° NC2022/0012870

- Reivindicación 4: La comunicación puede ocurrir a través de cualquier red de comunicaciones (115) conocida en la técnica, incluyendo, pero no limitado a redes cableadas, redes inalámbricas, redes Zigbee, redes Bluetooth, redes Z-wave, redes WiFi, redes WiMax, redes RF, redes de área local (LAN), redes de Internet, redes de área amplia (WAN), red de telefonía celular, redes telefónicas cableadas, redes inalámbricas de 900 MHz y redes satelitales. (Párr. 0029). El procesador (205) también está conectado a un transceptor (220) para enviar y recibir señales. En las implementaciones preferidas, el procesador (205) está conectado a una unidad de almacenamiento de datos (230). Esta unidad puede almacenar una cantidad predeterminada de datos recibidos de los sensores (215). Por ejemplo, puede almacenar datos durante un tiempo predeterminado (p. ej., un día, una semana o un mes), un número predeterminado de lecturas (p. ej., 10, 100 o 1000 lecturas) o hasta que el centro de operaciones le indique que los elimine. Además, la unidad de almacenamiento de datos (230) puede contener instrucciones que el procesador (205) debe ejecutar al recibir las instrucciones del centro de operaciones. En las implementaciones preferidas, el procesador (205) recopila al menos una parte de los datos almacenados en la unidad de almacenamiento (230) para su transmisión al centro de operaciones. (Párr. 0037)
- Reivindicación 6: En las realizaciones preferidas, el procesador (205) está conectado a una fuente de alimentación (235). Esta fuente puede ser un dispositivo capaz de alimentar el procesador (205) y los dispositivos conectados a él. Por ejemplo, la fuente de alimentación (235) puede ser una batería, un panel solar, una turbina eólica, una turbina hidráulica, líneas eléctricas o combinaciones de estos. En las realizaciones preferidas, también hay una fuente de alimentación de respaldo, como una batería. (Párr. 0038). Para un técnico medianamente versado en la materia resulta obvia la inclusión de puertos USB en sistemas de gestión de energía.

De igual manera, D2 divulga las características de las reivindicaciones dependientes así:

- Reivindicación 2: En una versión de la aplicación, el módulo de recopilación de datos (204) («DCM») comprende una computadora (210) con un microprocesador (212) y un medio legible por computadora (214) con periféricos de entrada/salida programables, configurado para gestionar todos los aspectos y funciones de los nodos sensores (200) como un sistema autónomo, incluyendo los detectores ambientales (202). En una versión, la computadora (210) del DCM (204) puede ser idealmente un microcontrolador de ultrabajo consumo («UMCU») diseñado para aplicaciones integradas. El UMCU cuenta con uno o más procesadores (212), junto con una memoria no volátil (214) codificada con instrucciones, así como una pequeña cantidad de memoria volátil (214) que se utiliza para almacenar datos ambientales en caso de pérdida de comunicación. En una versión, el DCM 204 puede incluir un reloj de tiempo real (216) que le permite generar informes de datos ambientales a intervalos definidos o en un momento dado. (Párr. 0049). como transmitir mensajes a través de un punto de acceso Wi-Fi local, a través de una red de área amplia de baja potencia (LPWAN) como LoRa/LoRaWAN, a través de un operador celular o un servicio general de radio por paquetes (GPRS), un operador satelital o mediante comunicación Bluetooth entre el nodo sensor (200) y un dispositivo móvil que retransmite el mensaje a la plataforma basada en la nube (103) a través de una aplicación móvil/computadora instalada. (Párr. 0056)
- Reivindicación 3: El módulo de telemetría de entrada (304) está configurado para recibir datos del módulo de telemetría del sensor (206). En ciertas versiones, el

Oficio N° 3039 de 25 de febrero de 2026

Ref. Expediente N° NC2022/0012870

módulo de telemetría de entrada (304) es utilizado por el dispositivo de enlace (302) para recibir de forma inalámbrica datos ambientales de varios nodos sensores (200). En una versión, el módulo de telemetría de entrada 304 incluye un receptor/concentrador LoRa configurado para proporcionar un enlace de comunicación hacia y desde los nodos sensores (200). (Párr. 0071)

- Reivindicación 5: Antes de importar un mensaje, la fuente de datos externa debe autenticarse en la plataforma en la nube (400). El ingestor gestiona el proceso de autenticación. Las fuentes de datos externas envían datos de autenticación al ingestor. Estos datos se presentan en forma de nombre de usuario y contraseña o una clave de autenticación. El ingestor recibe los datos de autenticación y los transmite al servicio de seguridad (426) para su autenticación. Este servicio compara los datos de autenticación con los del dispositivo almacenados en el servicio de almacenamiento (414). Si ambas fuentes de datos coinciden, el servicio de seguridad aprueba la solicitud de acceso de las fuentes de datos externas. (Párr. 0088)

Las reivindicaciones dependientes 2 a 6 no mencionan alguna característica que, junto con las características de la reivindicación independiente, aporte nivel inventivo al sistema de la reivindicación 1, por lo cual se considera que carecen de nivel inventivo.

6. Conclusión

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

Ítem	Documento	Reivindicaciones afectadas	Requisito que afecta
D1	US2010156632	1 a 6	Nivel inventivo
D3	US2019226898	1 a 6	Nivel inventivo

7. Respuesta a los argumentos del solicitante

Respuesta con respecto modificaciones a la solicitud en trámite

El solicitante manifiesta: “se presenta un nuevo capítulo reivindicatorio conformado por seis reivindicaciones, en las cuales se restringe la materia inicialmente reclamada para centrarla en el sistema que implementa en el Gateway un mecanismo de control de acceso basado en iniciar sesión en el servidor (59), cargar la lista del número de identificación de las tarjetas electrónicas autorizadas, recibir la trama del nodo por LoRa (58), separar los campos de información de la trama, comparar el número de identificación de la tarjeta electrónica con la lista y, según el resultado, formatear y enviar la información a la base de datos (60) o rechazar la trama y bloquear el dispositivo.”

En atención a lo manifestado por el solicitante quien presenta un nuevo capítulo reivindicatorio conformado por seis reivindicaciones, en el cual se restringe la materia inicialmente reclamada para centrarla en un sistema que implementa en el Gateway un mecanismo de control de acceso basado en: iniciar sesión en el servidor (59), cargar la lista de números de identificación de las tarjetas electrónicas autorizadas, recibir la trama del nodo por LoRa (58), separar los campos de información de la trama, comparar el número de identificación de la tarjeta con la lista y, según el resultado, formatear y enviar la información a la base de datos (60) o rechazar la trama y bloquear el dispositivo, esta Oficina procede a aceptar el nuevo pliego de reivindicaciones presentado.



Oficio N° 3039 de 25 de febrero de 2026

Ref. Expediente N° NC2022/0012870

El solicitante manifiesta: *“Se allega un nuevo capítulo reivindicatorio conformado por una única reivindicación independiente, en el cual se ha eliminado toda mención relacionada con marcas registradas, en particular “tipo Arduino”, de manera que ahora precisa únicamente características técnicas ya descritas”*

En atención a lo manifestado por el solicitante —quien allega un nuevo capítulo reivindicatorio conformado por una única reivindicación independiente, en el cual se elimina toda mención a marcas registradas, en particular la expresión “tipo Arduino”, precisando ahora únicamente características técnicas previamente descritas—, esta Oficina informa que la supresión de dichas referencias comerciales permite que las reivindicaciones cumplan con los requisitos formales correspondientes y, en consecuencia, resulten aceptables para su análisis de patentabilidad.

Respuesta con respecto no es una invención (art. 15 literal (f)) — “(...) las formas de presentar información”)

El solicitante manifiesta: *“La nueva reivindicación 1 ahora es de producto (sistema) y protege un Gateway con procesador (55) configurado para ejecutar una cadena técnica sobre tramas LoRa: iniciar sesión en el servidor (59), cargar la lista del número de identificación de las tarjetas electrónicas autorizadas, recibir la trama, separar sus campos, comparar el número de identificación de la tarjeta electrónica con la lista y decidir: formatear y enviar a base de datos (60) si es válido, o rechazar la trama y bloquear el dispositivo si no es válido”*

En atención a lo manifestado por el solicitante —quien indica que la nueva reivindicación independiente 1 está dirigida a un producto (sistema) y protege un Gateway con procesador (55) configurado para ejecutar una secuencia técnica de tratamiento de tramas LoRa, que comprende: iniciar sesión en el servidor (59), cargar la lista de números de identificación de tarjetas electrónicas autorizadas, recibir la trama, separar sus campos, comparar el número de identificación con dicha lista y, con base en el resultado, formatear y enviar la información a la base de datos (60) si es válida, o rechazar la trama y bloquear el dispositivo en caso contrario—, esta Oficina entiende y acepta la nueva caracterización de la reivindicación independiente 1.

Respuesta con respecto a la claridad

El solicitante manifiesta: *“Con esto, las reivindicaciones son claras y concisas, y se encuentran enteramente sustentadas por la descripción”*

Para esta Oficina es importante señalar que, una vez revisado el nuevo pliego de reivindicaciones, se observa que constituye una reestructuración más clara y concisa del objeto reivindicado, y que su contenido se encuentra debidamente sustentado en la descripción presentada. En tal sentido, cumple con los requisitos de claridad, concisión y soporte descriptivo exigidos.

El solicitante manifiesta: *“Ahora precisa únicamente características técnicas ya descritas, a saber: interfaz electrónica de expansión (47) adaptada a sensores (48); formación de tramas con número de trama, fecha y hora, número de identificación de la tarjeta electrónica, número de identificación del módulo LoRa (49), temperatura interna y datos del sensor; memoria microSD (50); enlace LoRa (58) nodo–Gateway; Wifi (56)/GSM (57) hacia servidor (59)/base de datos (60); y, en el Gateway, carga de la lista de identificaciones autorizadas, separación, comparación y acciones de formatear y enviar o rechazar y bloquear.”*

Oficio N° 3039 de 25 de febrero de 2026

Ref. Expediente N° NC2022/0012870

Cabe señalar que esta oficina informa que en el nuevo pliego de reivindicaciones se encuentra debidamente sustentado, tanto en la descripción presentada como en la información técnica considerada en los documentos D1 y D3 citados en el estado de la técnica, observándose correspondencia entre las características reivindicadas y dichos antecedentes.

Respuesta con respecto a la Unidad de invención

El solicitante manifiesta: *“se restringe el capítulo reivindicatorio al mismo concepto inventivo, referido a: control de acceso en el Gateway mediante carga de la lista del número de identificación de las tarjetas electrónicas autorizadas, separación de campos de la trama, comparación del número de identificación de la tarjeta electrónica con la lista, y decisión de formatear y enviar/rechazar y bloquear”*

Cabe señalar que el nuevo pliego de reivindicaciones define de manera más desarrollada un sistema con funciones de procesamiento orientadas específicamente al control de acceso en el Gateway, incluyendo etapas de carga de listas de identificación autorizadas, separación de campos de trama, comparación de identificadores y toma de decisiones operativas de envío, rechazo y bloqueo. Esta delimitación funcional permite reconocer con mayor precisión el carácter técnico del objeto reivindicado, por lo que resulta aceptable a la luz de las reivindicaciones actualmente presentadas.

Adicionalmente, se observa que el alcance técnico propuesto puede analizarse en correspondencia con la combinación de las enseñanzas de D1 y D3 citadas en el estado de la técnica, particularmente en lo relativo a comunicaciones inalámbricas, verificación de acceso y aplicación de mecanismos de control y protección del sistema. En consecuencia, el conjunto reivindicatorio se encuentra adecuadamente enmarcado frente a dichos antecedentes y permite continuar con el análisis técnico de patentabilidad.

Respuesta con respecto a la novedad

El solicitante manifiesta: *“A diferencia de D1 y D2, la solicitud define, con términos y secuencias operativas concretas, un sistema de detección temprana de inundación con (i) nodos sensores que arman “tramas” con campos específicos (número de trama, fecha y hora, número de identificación de la tarjeta electrónica, número de identificación del módulo LoRa, temperatura interna, datos del sensor) y almacenamiento local en microSD; y (ii) un Gateway que inicia sesión en un servidor para cargar la lista del número de identificación de las tarjetas electrónicas autorizadas, separa los campos de información de la trama recibida, compara el número de identificación de la tarjeta electrónica con dicha lista y, si no es válido, rechaza la trama y bloquea el dispositivo que intenta acceder al Gateway”*

Cabe señalar que el documento D1 describe sistemas orientados a la visualización y tratamiento de datos provenientes de sensores, en los cuales se emplean lecturas con marca de tiempo y su análisis en un centro de control. En particular, se indica que: “Además, en las realizaciones donde hay una marca de tiempo asociada a cada lectura, el centro de control puede determinar la dirección y velocidad aproximadas a la que se mueve el contaminante” (Párr. 0051).

Lo anterior evidencia que D1 ya contempla la obtención, registro y procesamiento de datos sensoriales con campos temporales específicos y su utilización para análisis operativo, dentro de arquitecturas de monitoreo remoto. En consecuencia, dichas enseñanzas constituyen un antecedente técnico pertinente que debe considerarse en la

Oficio N° 3039 de 25 de febrero de 2026

Ref. Expediente N° NC2022/0012870

evaluación comparativa del objeto reivindicado, de manera individual y en combinación con los demás documentos citados en el estado de la técnica.

El solicitante manifiesta: *“Aunque D1 describe arquitecturas de monitoreo amplias y redes genéricas y menciona que la comunicación puede usar redes conocidas (WiFi, celular, etc.), no enseña cargar desde un servidor la lista del número de identificación de las tarjetas electrónicas autorizadas, separar los campos de una trama LoRa para extraer el número de identificación de la tarjeta electrónica, compararlo con la lista y, ante no coincidencia, rechazar la trama y bloquear el dispositivo”*

Cabe señalar que el documento D1 sí contempla la asignación y uso de identificadores únicos asociados a los dispositivos de monitoreo y control dentro de la red. En particular, indica que a cada dispositivo se le asigna un identificador único y que cada comunicación puede incluir dicho identificador con el fin de reconocer el origen del mensaje y permitir su correcta gestión por el sistema o por el centro de operaciones (párr. 0032).

En este contexto, D1 ya enseña el empleo de identificadores de dispositivo incorporados en las comunicaciones del sistema y su utilización para fines de identificación y gestión de mensajes dentro de arquitecturas de monitoreo remoto. Por tanto, esta enseñanza constituye un antecedente técnico relevante que debe considerarse en el análisis comparativo de las características reivindicadas, en forma individual y en combinación con los demás documentos citados en el estado de la técnica.

El solicitante manifiesta: *“D2 se centra en detección de agua, temperatura y notificación, sin detallar formación de tramas con campos de identificación de tarjeta/módulo LoRa, ni carga de lista de autorizados en el Gateway, ni bloqueo de dispositivos ante identificaciones no válidas”*

Cabe señalar que si bien el documento D2 no hace referencia a esta característica, el documento D3 incluido en este requerimiento describe: De manera similar, el sensor de El módulo de telemetría (204) puede transmitir los datos ambientales al dispositivo de enlace (302) o a la plataforma basada en la nube (400) a través de varias formas de infraestructura de protocolo de comunicación inalámbrica (317), como la transmisión de mensajes a través de un punto de acceso Wi-Fi local, a través de una red de área amplia de baja potencia (LPWAN) como LoRa/LoRaWAN, a través de un operador celular o un servicio general de radio por paquetes (GPRS) (...) (Párr. 0056)

Esta divulgación evidencia que D3 sí contempla comunicación LoRa. En consecuencia, tales enseñanzas constituyen un antecedente técnico pertinente dentro del estado de la técnica y deben ser consideradas en la evaluación comparativa de las características reivindicadas, particularmente en lo relativo a la arquitectura de comunicación y transmisión de datos del sistema.

La Oficina observa que el solicitante manifiesta: *“D2 se centra en detección de agua, temperatura y notificación, sin detallar formación de tramas con campos de identificación de tarjeta/módulo LoRa, ni carga de lista de autorizados en el Gateway, ni bloqueo de dispositivos ante identificaciones no válidas”*.

No obstante, resulta pertinente señalar que, con la incorporación del de D3 como parte del estado de la técnica, se evidencia que las características que el solicitante considera ausentes en D2 sí se encuentran divulgadas de manera expresa o implícita.

En efecto, D3 describe en su memoria descriptiva mecanismos de identificación de dispositivos en redes LoRa, incluyendo la transmisión de información identificativa en las

Oficio N° 3039 de 25 de febrero de 2026

Ref. Expediente N° NC2022/0012870

tramas de comunicación, la validación de dispositivos en el Gateway mediante listas preconfiguradas o registros autorizados, así como procedimientos de rechazo o bloqueo ante identificaciones no válidas.

Por consiguiente, para un técnico medianamente versado en la materia, la combinación de D2 con D3 no implica actividad inventiva, dado que D3 complementa de manera directa las supuestas deficiencias técnicas alegadas respecto de D2, aportando precisamente las funcionalidades relacionadas con autenticación, identificación y control de acceso en redes LoRa.

En este sentido, la materia reivindicada no supera el requisito de nivel inventivo, al derivarse de manera evidente de la combinación de D1 con D3 dentro del estado de la técnica.

Respuesta con respecto al nivel inventivo

El solicitante manifiesta: *“la incorporación de D2 tampoco suple las carencias anteriores. D2 se ocupa de notificación de inundación y sensores de temperatura y agua, con mención a enlaces cableados (USB/Ethernet), pero no describe que el Gateway inicie sesión en el servidor (59) para cargar la lista de identificaciones autorizadas, tampoco sugiere separar los campos de la trama LoRa (58) para tomar el número de identificación de la tarjeta electrónica ni compararlo con una lista, y mucho menos contempla rechazar la trama y bloquear el dispositivo.”*

No obstante, esta Oficina considera que tales alegaciones no desvirtúan la falta de nivel inventivo cuando se analiza la combinación del documento D1 con el documento US20190226898 (D3).

En efecto, D3 divulga expresamente mecanismos de autenticación de dispositivos mediante comparación con datos almacenados en una base de datos. Así, en su memoria descriptiva señala:

“Antes de importar un mensaje, la fuente de datos externa debe autenticarse en la plataforma en la nube (400). (...) El servicio de seguridad (426) compara los datos de autenticación con los datos de autenticación del dispositivo almacenados en el servicio de almacenamiento (414)” (Párr. 0088).

Lo anterior evidencia que D3 sí contempla la autenticación basada en la comparación de credenciales con una base de datos de dispositivos autorizados, lo cual se corresponde funcionalmente con una “lista de identificaciones autorizadas”, aun cuando dicha verificación se realice en el servidor y no estrictamente en el Gateway.

Asimismo, D3 establece que:

“Si no se concede la autorización, el servicio de ingesta (410) rechazará cualquier mensaje entrante del dispositivo no autorizado.” (Párr. 0136).

Por tanto, el documento sí contempla el rechazo de mensajes provenientes de dispositivos no autenticados, lo cual se aproxima directamente a la característica alegada de “rechazar la trama y bloquear el dispositivo” cuando la identificación no es válida.

Adicionalmente, D3 describe procesos de separación o procesamiento de mensajes recibidos:

Oficio N° 3039 de 25 de febrero de 2026

Ref. Expediente N° NC2022/0012870

“El servicio de procesamiento de flujo (412) divide el mensaje en eventos ambientales discretos. (...) El paso (918) separa estas lecturas (...) en registros de eventos individuales.” (Párr. 0151).

Aunque dicho procesamiento se realiza en la nube, esta divulgación evidencia la enseñanza técnica de descomponer o “parsear” mensajes para trabajar con sus campos individuales, lo cual incluye necesariamente la extracción de información identificativa contenida en la trama.

Finalmente, D3 señala:

“En ciertas versiones, al iniciarse, los dispositivos de puerta de enlace (302) se configurarán para ser autenticados primero por la plataforma en la nube (400) antes de que el dispositivo de puerta de enlace (302) esté autorizado a intercambiar datos...” (Párr. 0131).

Con ello se demuestra que el Gateway debe autenticarse ante el servidor antes de intercambiar datos, lo cual se corresponde con el concepto alegado de “iniciar sesión” o realizar un proceso previo de validación frente a la plataforma.

En consecuencia, para un técnico medianamente versado en la materia, la combinación de D1 con D3 conduce de manera evidente a la implementación de mecanismos de autenticación, comparación con bases de datos de dispositivos autorizados, procesamiento de mensajes para extracción de campos y rechazo de comunicaciones no autorizadas.

Por tanto, las características invocadas por el solicitante no configuran una actividad inventiva, sino que resultan de la aplicación evidente de enseñanzas ya divulgadas en el estado de la técnica.

El solicitante manifiesta: *“Ni D1 aporta un control de acceso por identificación de tarjeta, ni D2 sugiere bloqueo a nivel de Gateway; por tanto, la hipótesis de combinación requeriría reconstrucción ex post facto apoyada en la propia solicitud, y no en una motivación técnica derivable de D1 o D2”*

Cabe señalar que el documento D1 sí aporta enseñanzas técnicas relacionadas con mecanismos de identificación de dispositivos y control de acceso dentro de sistemas de monitoreo y comunicación inalámbrica. En particular, se indica que: “En las implementaciones preferidas, a cada dispositivo de monitoreo (110) y a cada dispositivo de control (111) se le asigna un identificador único. Este identificador único puede estar relacionado con la ubicación geográfica, la dirección, el orden de instalación o cualquier otro método de identificación. Además, los diferentes tipos de dispositivos (110) y (111) pueden tener identificadores únicos. Por ejemplo, el identificador de todos los medidores de agua puede comenzar con WM, mientras que el de todos los detectores de fugas puede comenzar con LD. Cada comunicación entre los dispositivos (110) y (111) puede incluir el identificador único para que el mensaje sea recibido por el dispositivo (110) o (111) correcto, o el centro de operaciones (105) pueda determinar desde dónde se envió el mensaje.” (Párr. 0032).

Asimismo, D1 establece expresamente medidas de protección y control de acceso al sistema al señalar que: “Preferiblemente, la comunicación se realiza mediante un componente inalámbrico, por ejemplo, desde el dispositivo de monitoreo remoto o el dispositivo de control a una instalación de monitoreo regional o a monitores distribuidos. También es preferible que las comunicaciones estén protegidas o cifradas, de modo que

Oficio N° 3039 de 25 de febrero de 2026

Ref. Expediente N° NC2022/0012870

el sistema de comunicaciones no pueda ser monitoreado por terceros desconocidos. El acceso al sistema se otorga preferiblemente mediante nombres de usuario y contraseñas, aunque se pueden emplear métodos de cifrado adicionales o alternativos.” (Párr. 0027).

En consecuencia, D1 ya contempla el uso de identificadores únicos en las comunicaciones y la aplicación de mecanismos de control de acceso y protección del sistema. Tales enseñanzas proporcionan motivación técnica suficiente para considerar verificaciones de identidad y restricciones de acceso a nivel de sistema, por lo que su combinación con D2 no implica una reconstrucción ex post facto, sino una integración técnicamente derivable a partir del estado de la técnica.

El solicitante manifiesta: *“la disposición y/o configuración particular de las características técnicas de la reivindicación 1 modificada, iniciar sesión en el servidor (59) para cargar la lista del número de identificación de las tarjetas electrónicas autorizadas, separar los campos de información de la trama recibida por LoRa (58) para tomar el número de identificación de la tarjeta electrónica y compararlo con la lista, y decidir para: formatear y enviar a la base de datos (60) cuando es válido o rechazar la trama y bloquear el dispositivo cuando no es válido es la que permite formular correctamente dicho problema técnico a nivel de Gateway.”*

Cabe señalar que el documento D1 ya describe un sistema que incorpora mecanismos de identificación de dispositivos y control de acceso dentro de arquitecturas de monitoreo con comunicaciones inalámbricas. En particular, establece que: “En las implementaciones preferidas, a cada dispositivo de monitoreo (110) y a cada dispositivo de control (111) se le asigna un identificador único. Este identificador único puede estar relacionado con la ubicación geográfica, la dirección, el orden de instalación o cualquier otro método de identificación. Además, los diferentes tipos de dispositivos (110) y (111) pueden tener identificadores únicos. Por ejemplo, el identificador de todos los medidores de agua puede comenzar con WM, mientras que el de todos los detectores de fugas puede comenzar con LD. Cada comunicación entre los dispositivos (110) y (111) puede incluir el identificador único para que el mensaje sea recibido por el dispositivo (110) o (111) correcto, o el centro de operaciones (105) pueda determinar desde dónde se envió el mensaje.” (Párr. 0032).

Asimismo, D1 también prevé expresamente mecanismos de protección y control de acceso al sistema, al indicar que: “Preferiblemente, la comunicación se realiza mediante un componente inalámbrico, por ejemplo, desde el dispositivo de monitoreo remoto o el dispositivo de control a una instalación de monitoreo regional o a monitores distribuidos. También es preferible que las comunicaciones estén protegidas o cifradas, de modo que el sistema de comunicaciones no pueda ser monitoreado por terceros desconocidos. El acceso al sistema se otorga preferiblemente mediante nombres de usuario y contraseñas, aunque se pueden emplear métodos de cifrado adicionales o alternativos.” (Párr. 0027).

Asimismo D3 señala: De manera similar, el sensor del módulo de telemetría (204) puede transmitir los datos ambientales al dispositivo de enlace (302) o a la plataforma basada en la nube (400) a través de varias formas de infraestructura de protocolo de comunicación inalámbrica (317), como la transmisión de mensajes a través de un punto de acceso Wi-Fi local, a través de una red de área amplia de baja potencia (LPWAN) como LoRa/LoRaWAN, a través de un operador celular o un servicio general de radio por paquetes (GPRS) (...) (Párr. 0056). Y por consiguiente a: El módulo de telemetría de entrada (304) está configurado para recibir datos del módulo de telemetría del sensor (206). En ciertas versiones, el módulo de telemetría de entrada (304) es utilizado por el dispositivo de enlace (302) para recibir de forma inalámbrica datos ambientales de varios nodos sensores 200. En una versión, el módulo de telemetría de entrada (304) incluye

Oficio N° 3039 de 25 de febrero de 2026

Ref. Expediente N° NC2022/0012870

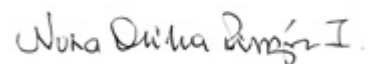
un receptor/concentrador LoRa configurado para proporcionar un enlace de comunicación hacia y desde los nodos sensores (200). (Párr. 0071)

En consecuencia, la verificación de identidad de dispositivos, la validación de comunicaciones entrantes y la aplicación de medidas de restricción de acceso a nivel de sistema ya se encuentran contempladas en el estado de la técnica. Por tanto, la configuración funcional planteada a nivel de Gateway debe analizarse como una implementación específica de controles de identificación y acceso ya conocidos, y no como un planteamiento técnico aislado carente de antecedentes.

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.



Nubia Milena Pinzon Ibañez
DIRECTORA DE NUEVAS CREACIONES (E)

Oficio N° 3039 de 25 de febrero de 2026

Ref. Expediente N° NC2022/0012870

INFORME DE BÚSQUEDA
EXAMEN DE PATENTABILIDAD

Solicitud No.		Examen de patentabilidad							
NC2022/0012870		1°	-	2°	X	3°	-	Revoca	-
Fecha de determinación estado de la técnica (DD/MM/AÑO)				Prioridad		Presentación			
09/09/2022				-		X			
Solicitante									
CORPORACIÓN UNIVERSITARIA MINUTO DE DIOS - UNIMINUTO									
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 6
Palabras clave utilizadas	Processor, sensor, interface, wifi, gsm, server, database, frame, microSD, usb port, solar panels, power management subsystem, identification, alert, LoRa, LoRaWAN.
Clasificaciones utilizadas para la búsqueda	CIP: H04W 4/38, H04W 12/121, H04Q 3/00, H04Q 11/00, G05B 9/00, G05B 19/00, G05B 23/00

DOCUMENTOS CONSIDERADOS RELEVANTES (Documentos patente, Literatura no patente (LNP): Artículos, catálogos, etc.)					
Informes de búsqueda / Bases de datos consultadas	N° de solicitud de patente / N° de patente / Autor LNP ⁽¹⁾	Fecha de Publicación /Presentación (DD/MM/AAAA)	Reivindicaciones /Secuencias afectadas	Citas relevantes del estado de la técnica	Categoría del documento citado ⁽²⁾
SIPI	NC2018/0013181	19/02/2019	-	-	A
Patbase	US2018375680	27/12/2018	-	-	A
	US2023049699	16/02/2023	-	-	A
	US2023296480	21/09/2023	-	-	A
	US2018321033	08/11/2018	-	-	A
	AU2020102301	29/10/2020	-	-	A
	AU2020102711	03/12/2020	-	-	A
	US2017294101	12/10/2017	-	-	A
	US2010156632	24/06/2010	1 a 6	(Párr. 0026) (Párr. 0027) (Párr. 0029) (Párr. 0032) (Párr. 0036) (Párr. 0037) (Párr. 0038) (Párr. 0059)	Y
	US2019226898	25/07/2019	1 a 6	(Párr. 0042) (Párr. 0051) (Párr. 0056) (Párr. 0059) (Párr. 0061) (Párr. 0071) (Párr. 0072) (Párr. 0080) (Párr. 0088) (Párr. 0094) (Párr. 0096) (Párr. 0114) (Párr. 0136) (Reiv. 1) (Reiv. 4)	Y
US2022180724	09/06/2022	-	-	A	
Orbit	CN111107675	02/03/2021	-	-	A
Espacenet	US20220163959	26/05/2022	-	-	A
Googlepatent	AU2020392228	14/07/2022	-	-	A
⁽¹⁾ Cita completa literatura no patente					



Oficio N° 3039 de 25 de febrero de 2026

Ref. Expediente N° NC2022/0012870

(LNP)	
Apellido, A. A. (Fecha). Título del artículo. <i>Nombre de la revista. Volumen</i> (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: (23/02/2026)	

