

REPÚBLICA DE COLOMBIA
SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO

Resolución N° 32480

Ref. Expediente N° NC2022/0007161

Por la cual se deniega una Patente de Modelo de utilidad

LA DIRECTORA DE NUEVAS CREACIONES (E)

en ejercicio de sus facultades legales, en especial de las conferidas en el numeral 5° del artículo 20 del Decreto 4886 de 2011, y

CONSIDERANDO

Que mediante escrito radicado en esta Superintendencia el 26 de mayo de 2022 con el N° NC2022/0007161, CENTRO DE INVESTIGACION Y DESARROLLO TECNOLÓGICO DE LA INDUSTRIA ELECTRO ELECTRÓNICA Y TIC CIDEI presentó la solicitud de patente de invención titulada “SISTEMA Y MÉTODO PARA LA INTRUSIÓN DE SEÑALES DE COMUNICACIÓN Y GEOLOCALIZACIÓN DE DRONES”.

Que la solicitud fue publicada en la Gaceta de la Propiedad Industrial N° 981 el 29 de noviembre de 2022, sin que se hubieran presentado oposiciones por parte de terceros.

Que, mediante escrito radicado bajo el N° NC2025/0016999 el 4 de diciembre de 2025, el solicitante solicitó conversión de modalidad de patente de invención a patente de modelo de utilidad. Se acepta el cambio de modalidad, comoquiera que se ajusta a las prescripciones contenidas en los artículos 34 y 35 de la Decisión 486 y el artículo 2.2.2.19.2.2 del Decreto 1074 de 2015. Por lo tanto, la presente decisión hace referencia a una patente de modelo de utilidad.

Que realizado el examen de fondo mediante Oficio No. 4023 de 9 de marzo de 2026, se requirió al solicitante en los términos del artículo 45 de la Decisión 486 de la Comisión de la Comunidad Andina para que presentara respuesta a las observaciones de carácter técnico, relacionadas con la patentabilidad o cumplimiento de los requisitos establecidos por esta Decisión para la concesión de la patente.

Que, mediante escrito radicado bajo el N° NC2022/0007161 el 15 de abril de 2026, el solicitante respondió oportunamente el requerimiento formulado sin presentar nuevo capítulo reivindicatorio. Por lo tanto, se tendrá en cuenta el capítulo reivindicatorio presentado con el radicado N° NC2022/0007161 el 4 de diciembre de 2025.

Teniendo en cuenta lo dispuesto en el artículo 85 de la Decisión 486 expedida por la Comisión de la Comunidad Andina: *“Son aplicables a las patentes de modelo de utilidad, las disposiciones sobre patentes de invención contenidas en la presente Decisión en lo que fuere pertinente, salvo en lo dispuesto con relación a los plazos de tramitación, los cuales se reducirán a la mitad. Sin perjuicio de lo anterior, el plazo establecido en el artículo 40 quedará reducido a doce meses.”*

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

Asimismo, el artículo 81 de la Decisión 486 indica que: *“Se considera modelo de utilidad, a toda nueva forma, configuración o disposición de elementos, de algún artefacto,*

Ref. Expediente N° NC2022/0007161

herramienta, instrumento, mecanismo u otro objeto o de alguna parte del mismo, que permita un mejor o diferente funcionamiento, utilización o fabricación del objeto que le incorpore o que le proporcione alguna utilidad, ventaja o efecto técnico que antes no tenía. Los modelos de utilidad se protegerán mediante patentes”.

Que las reivindicaciones 1 y 2 incluidas en el radicado bajo el N° NC2022/0007161 el 4 de diciembre de 2025, no cumplen los requisitos indicados. Lo anterior, de acuerdo con las siguientes consideraciones:

Objeto de la invención

El problema planteado consiste en la necesidad de proporcionar un dispositivo para la intrusión de señales de comunicación y geolocalización de drones comerciales dada la utilización de drones para atentar contra la seguridad de infraestructura crítica o para ejecutar acciones ilegales.

Para resolver dicho problema técnico, la solicitud en estudio plantea un dispositivo para la intrusión de señales de comunicación y para la intrusión a señales de geolocalización de drones que comprende: dos conjuntos, con computadores de placa sencilla, un conjunto de módulo WiFi para realizar el ataque y bloquear todos los dispositivos que estén conectados a un canal específico de WiFi a través de dos bandas de frecuencia; y un conjunto de módulo de bloqueo del GPS para abrir una terminal de comandos para el ataque y cargar las coordenadas falsas en un nuevo archivo que utiliza las características de seguridad del dron en su contra y forzar su aterrizaje o desvío por medio de un módulo de radio SDR y un módulo reloj TCXO externo; fijados en un encerramiento con pre-amplificadores de señal, amplificadores de señal y un switch ethernet de conexión a los computadores de placa sencilla, conectado a su vez a un Computador portátil que se ejecuta con dos bloques de procesamiento independientes y direcciones IP diferentes para activar la intrusión de una o de las dos señales de comunicación (WiFi y GPS).

Determinación del Estado de la Técnica

La fecha para determinar el estado de la técnica es el 26 de mayo de 2022, que corresponde a la fecha de presentación.

Consultadas las fuentes de información con que se cuenta, se encontró el siguiente documento que anticipa el objeto de esta solicitud:

Ítem	Documento	Título	Fecha de publicación
D4	CN 110719136	“Unmanned aerial vehicle interference deception system and unmanned aerial vehicle defense system”	21 de enero de 2020

D1¹ divulga un sistema de engaño de interferencias de vehículos aéreos no tripulados y un sistema de defensa de vehículos aéreos no tripulados, que comprenden específicamente: un sistema de engaño de interferencias de vehículos aéreos no tripulados, una máquina todo en uno de seguimiento fotoeléctrico, interferencia de radio y engaño de GPS y un sistema de defensa de vehículos aéreos no tripulados; y el método de captura de engaño de GPS de vehículos aéreos no tripulados y el método de posicionamiento de volante de vehículos aéreos no tripulados se proporcionan con base en el sistema de defensa de vehículos aéreos no tripulados (Resumen).

¹<https://patents.google.com/patent/CN110719136A/en?q=CN110719136>



Ref. Expediente N° NC2022/0007161

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.

Novedad

Teniendo en cuenta lo señalado en el artículo 16 de la Decisión 486 de 2000 de la Comisión de la Comunidad Andina, la reivindicación independiente 1 (NC2022/0007161 del 4 de diciembre de 2025) refiere a: *“Dispositivo para la intrusión de señales de comunicación y para la intrusión a señales de geolocalización de drones que comprende (...)”*. A continuación, se presenta la tabla comparativa entre el objeto reivindicado y los documentos encontrados en el estado de la técnica:

CARACTERÍSTICAS ESENCIALES	D4
Dispositivo para la intrusión de señales de comunicación y para la intrusión a señales de geolocalización de drones que comprende los siguientes elementos y características:	(...) un sistema de engaño de interferencias de vehículos aéreos no tripulados y un sistema de defensa de vehículos aéreos no tripulados (...) interferencia de radio y engaño de GPS y un sistema de defensa de vehículos aéreos no tripulados (...) (Resumen)
Dos conjuntos, con computadores de placa sencilla (2w, 2G).	(...) dispositivo front-end y dispositivo back-end (...) (Reiv. 1)
Un conjunto de módulo Wifi (11) para realizar el ataque y bloquear todos los dispositivos que estén conectados a un canal específico de Wifi a través de dos bandas de frecuencia.	(...) un módulo de interferencia de radio de 2,4 G y un módulo de interferencia de radio de 5,8 G que están conectados respectivamente a la parte posterior del controlador del interruptor de interferencia (...) (Reiv. 2)
Un conjunto de módulo de bloqueo del GPS (sistema de posicionamiento global) (12) para abrir una terminal de comandos para el ataque y cargar las coordenadas falsas en un nuevo archivo que utiliza las características de seguridad del dron en su contra y forzar su aterrizaje o desvío por medio de un módulo de radio SDR y un módulo reloj TCXO externo.	(...) la unidad de engaño de interferencia de radio se utiliza para generar y transmitir una señal de interferencia de comunicación de radio, una señal de interferencia de banda de frecuencia GPS y una señal de engaño GPS del vehículo aéreo no tripulado a través de la antena de radiofrecuencia direccional; la señal de interferencia de banda de frecuencia GPS se utiliza para interferir la comunicación entre el vehículo aéreo no tripulado y el GPS; la señal de interferencia de comunicación de radio se utiliza para interferir la comunicación entre el vehículo aéreo no tripulado y el extremo de control remoto (...) (Reiv. 1) (...) la parte de generación de la señal de engaño GPS de la unidad de engaño de interferencia de radio consta de un generador de radio de software conectado al conmutador de red frontal y un módulo de amplificación de potencia de radiofrecuencia de 1,5 G conectado a la parte posterior del generador de radio de software (...) (Reiv. 2) Aunque el documento no mencione explícitamente los módulos de reloj TCXO, los mismos se



Ref. Expediente N° NC2022/0007161

	encuentran implícitamente en el sistema GPS. Dado que el oscilador de cuarzo de alta precisión utiliza un circuito especial para compensar las variaciones de frecuencia causadas por cambios de temperatura, siendo ideales para GPS, telecomunicaciones y equipos que requieren sincronización precisa.
Fijados en un encerramiento (9) con pre-amplificadores de señal (5), amplificadores de señal.	(...) la señal de interferencia de radiocomunicación generada por la unidad de engaño de interferencias de radio se divide en una señal de interferencia de baja frecuencia y una señal de interferencia de alta frecuencia. La señal de interferencia de baja frecuencia es generada por un generador de radio de software conectado a un conmutador de red frontal, se envía a un módulo de amplificación de potencia de baja frecuencia para su amplificación y se transmite mediante una antena de radiofrecuencia direccional ultra ancha de baja frecuencia. La señal de interferencia de alta frecuencia es generada por un generador de radio de software conectado a un conmutador de red frontal, se envía a un módulo de amplificación de potencia de alta frecuencia para su amplificación y se transmite mediante una antena de radiofrecuencia direccional ultra ancha de alta frecuencia (Reiv. 3)
Y un switch ethernet (1) de conexión a los computadores de placa sencilla, conectado su vez a un Computador portátil (10) que se ejecuta con dos bloques de procesamiento independientes y direcciones IP diferentes para activar la intrusión de una o de las dos señales de comunicación (Wifi y GPS).	(...) un conmutador de red front-end y un módulo de alimentación (...) el sistema de soporte del servo está en comunicación de datos con la computadora back-end a través del conmutador de red frontal. (Reiv. 1) (...) la parte de generación de señales de interferencia de comunicación por radio y señales de interferencia de banda de frecuencia GPS de la unidad de engaño de interferencia de radio consta de un controlador de interruptor de interferencia conectado a un conmutador de red frontal, un módulo de interferencia de radio de 1,5 G, un módulo de interferencia de radio de 2,4 G y un módulo de interferencia de radio de 5,8 G que están conectados respectivamente a la parte posterior del controlador de interruptor de interferencia (...) (Reiv. 2)

De acuerdo con la comparación realizada anteriormente se concluye que la materia de la reivindicación 1 no es nueva.

Así mismo, D4 divulga las características de las reivindicaciones dependientes de la siguiente manera:

- Reivindicación 2: (...) la señal de interferencia de radiocomunicación generada por la unidad de engaño de interferencias de radio se divide en una señal de interferencia de baja frecuencia y una señal de interferencia de alta frecuencia. La señal de interferencia de baja frecuencia es generada por un generador de radio de software conectado a un conmutador de red frontal, se envía a un módulo de amplificación de potencia de baja frecuencia para su amplificación y se transmite mediante una antena de radiofrecuencia direccional ultra ancha de baja frecuencia. La señal de interferencia de alta frecuencia es generada por un generador de radio de software conectado a un conmutador de red



Ref. Expediente N° NC2022/0007161

frontal, se envía a un módulo de amplificación de potencia de alta frecuencia para su amplificación y se transmite mediante una antena de radiofrecuencia direccional ultra ancha de alta frecuencia (Reiv. 3).

En consecuencia, La reivindicación dependiente 2 tampoco cumple con el requisito de novedad.

Respuesta a los argumentos del solicitante

En lo referente a los argumentos del solicitante con relación a la novedad de las reivindicaciones 1 y 2 bajo estudio en donde manifestó que el documento D4 menciona un dispositivo front-end y un dispositivo back-end, sin embargo, no describe una arquitectura con dos mecanismos independientes especializados para tipos distintos de intrusión, ni el control simultáneo de dichos sistemas desde un computador externo mediante direccionamiento IP independiente. Por su parte, la solicitud es un dispositivo que comprende dos computadores de placa sencilla independientes, cada uno dedicado a un tipo específico de intrusión: - Uno para el ataque WiFi, - Uno para el ataque GPS. Cada uno opera con direcciones IP diferentes y bloques de procesamiento. Por lo tanto, la arquitectura reivindicada presenta una configuración estructural distinta, más ágil por ser dedicada en cada placa independiente, sin interferencia y con procesamiento independiente pero simultáneo; estructura que difiere en ejecución y velocidad de procesamiento de la señal como está estructurado D4.

De lo anterior, esta Oficina se permite indicar que las reivindicaciones son una parte esencial de la solicitud pues definen la invención a proteger y delimitan el alcance de esa protección, tal y como lo establece el Artículo 51 de la Decisión 486: *“Artículo 51.- El alcance de la protección conferida por la patente estará determinado por el tenor de las reivindicaciones. La descripción y los dibujos, o en su caso, el material biológico depositado, servirán para interpretarlas.”* Del Artículo 30 de la Decisión 486 se derivan tres requisitos fundamentales de las reivindicaciones: que sean claras, concisas y que tengan sustento en la descripción, de tal forma que: se puedan comparar y diferenciar del estado de la técnica con el fin de verificar los requisitos de patentabilidad; y se pueda determinar sin ambigüedad hasta dónde llegan los derechos del titular de la patente. Estos requisitos se aplican a cada reivindicación individualmente, así como al conjunto de todas.

Así las cosas, las reivindicaciones deben definir de manera clara el objeto para el que se solicita la protección porque de acuerdo con la claridad de las reivindicaciones será posible determinar si la invención es nueva, inventiva y susceptible de aplicación industrial. Adicionalmente, las reivindicaciones deben interpretarse de la misma forma, tanto a los efectos de la búsqueda como a los del examen. No obstante, las reivindicaciones deben ser claras por sí mismas. Asimismo, las reivindicaciones deben contener todas las características técnicas esenciales de la invención. Ellas definen la solución al problema técnico que intenta resolver la invención. Si el estado de la técnica más cercano contiene todas las características de la reivindicación, tanto técnicas como no técnicas, el objeto de la reivindicación no es nuevo. En consecuencia, la solicitud no es patentable.

Es así como en relación con el primer argumento en el que el solicitante afirma que su dispositivo presenta dos computadores de placa sencilla independientes, mientras que D4 describe un sistema con dispositivo front-end y back-end, se tiene que el mismo no es de recibo por parte de esta Oficina, en la medida que la comparación realizada en el examen muestra que ambos sistemas cumplen la misma función, la cual es ejecutar procesos de interferencia y engaño de señales mediante módulos conectados a un conmutador de red. La diferencia alegada es meramente de implementación, sin embargo, bajo el tenor de las

Ref. Expediente N° NC2022/0007161

reivindicaciones dicho concepto no es novedoso frente al documento del estado de la técnica. La normativa andina exige que la novedad se fundamente en características técnicas no divulgadas, y en este caso la función esencial ya está anticipada por D4, por lo mismo tales argumentos son insuficientes para otorgar las reivindicaciones 1 y 2.

En lo referente a los argumentos del solicitante con relación a la novedad de las reivindicaciones 1 y 2 bajo estudio en donde manifestó que el dispositivo propuesto incluye un mecanismo de ciberataque WiFi que consiste en bloquear dispositivos conectados a un canal específico de WiFi, lo cual permite dirigir la intrusión únicamente hacia los enlaces de comunicación del dron. D4, por el contrario, describe módulos de interferencia de radio de 2,4 G y 5,8 G conectados a un controlador de interruptor, operando mediante barrido o interferencia de banda ancha, sin la capacidad de seleccionar, monitorear o bloquear de forma dirigida un canal específico de comunicación activa. Esta diferencia estructural en el módulo de ataque permite una neutralización específica que D4 no enseña ni sugiere.

De lo anterior, esta Oficina se permite indicar que la falta de novedad aún continúa siendo pertinente, en la medida que la característica reivindicada menciona un conjunto de módulo WiFi para realizar el ataque y bloquear todos los dispositivos que estén conectados a un canal específico de WiFi a través de dos bandas de frecuencia. Por su parte, el documento D4 anticipa esta característica al mencionar (...) un módulo de interferencia de radio 2,4 G y un módulo de interferencia de radio de 5,8 G que están conectados respectivamente a la parte posterior del controlador del interruptor de interferencia (...) (Reiv. 2), lo que en esencia implica que el sistema ya contempla la interferencia en ambas bandas de frecuencia utilizadas por drones comerciales. Aunque el solicitante argumenta que su dispositivo permite bloquear un canal específico, la interferencia en bandas de 2,4 y 5,8 GHz divulgada en D4 abarca los mismos canales de comunicación. Es así como con relación al segundo argumento, se tiene que el mismo no es de recibo por parte de esta Oficina, en la medida que la mencionada característica carece de novedad, por lo mismo tales argumentos son insuficientes para otorgar las reivindicaciones 1 y 2.

En lo referente a los argumentos del solicitante con relación a la novedad de las reivindicaciones 1 y 2 bajo estudio en donde manifestó que el dispositivo reivindicado utiliza un mecanismo específico de intrusión GPS basado en el envío de coordenadas falsas que activan mecanismos de seguridad del firmware del dron, generando un aterrizaje automático o retorno a origen. En contraste, el documento D4 describe la generación de señales de interferencia y engaño GPS de forma general, pero no divulga el uso de los mecanismos de geofencing del firmware del dron como parte del método de neutralización. Esta diferencia constituye una distinción funcional relevante, ya que la invención no solo emite señales falsas, sino que interactúa con la lógica de seguridad interna del UAV para forzar un comportamiento controlado, aspecto no derivable de la configuración o funcionamiento de D4.

De lo anterior, esta Oficina se permite indicar que la falta de novedad aún continúa siendo pertinente, en la medida que el argumento de que la invención explota el firmware del dron para inducir aterrizaje automático no desvirtúa la anticipación. D4 divulga expresamente la generación de señales falsas de GPS para engañar al UAV, lo cual abarca la misma finalidad: alterar el comportamiento del dron mediante información de posicionamiento manipulada. La forma específica de interacción con el firmware no constituye un elemento técnico nuevo, sino una consecuencia del mismo principio de engaño GPS ya divulgado. Es así como, en relación con el tercer argumento, se tiene que el mismo no es de recibo por parte de esta Oficina, en la medida que se reitera que las características reivindicadas

Ref. Expediente N° NC2022/0007161

son anticipadas por el documento D4, por lo mismo tales argumentos son insuficientes para otorgar las reivindicaciones 1 y 2.

En lo referente a los argumentos del solicitante con relación a la novedad de las reivindicaciones 1 y 2 bajo estudio en donde manifestó que el examen señala que el módulo de reloj TCXO se encuentra implícito en el sistema GPS del documento D4. Sin embargo, esta afirmación no puede considerarse válida desde el punto de vista técnico, dado que el documento D4 no menciona explícitamente dicho componente y: - Los sistemas GPS pueden operar con distintos tipos de osciladores. - El uso de un TCXO no es obligatorio ni inherente a todos los sistemas GPS. Por lo tanto, no es posible considerar que esta característica esté divulgada de forma implícita en el estado de la técnica. Conforme a la Guía de la SIC, la divulgación implícita solo opera cuando el experto en la materia puede derivar el elemento de manera directa e inequívoca sin necesidad de experimentación o suposición. D4 carece de tal enseñanza.

El solicitante cuestiona la divulgación implícita del TCXO en D4. Sin embargo, el examen técnico concluyó correctamente que los sistemas GPS requieren osciladores de alta precisión para garantizar sincronización, siendo el TCXO una opción estándar en la técnica. La jurisprudencia y la Guía de la SIC reconocen que la divulgación implícita aplica cuando el experto en la materia puede derivar el elemento de manera directa e inequívoca, como ocurre en este caso. Es así como, con relación al cuarto argumento, se tiene que el mismo no es de recibo por parte de esta Oficina, por lo mismo tales argumentos son insuficientes para otorgar las reivindicaciones 1 y 2.

En lo referente a los argumentos del solicitante con relación a la novedad de las reivindicaciones 1 y 2 bajo estudio en donde manifestó que el dispositivo reivindicado incluye una interfaz gráfica de control que permite gestionar de manera simultánea los ataques WiFi y GPS desde un computador externo, permitiendo la operación remota del dispositivo. El documento D4 describe módulos de interferencia de radio de baja y alta frecuencia, pero no divulga una arquitectura de control basada en interfaz gráfica con coordinación simultánea de dos sistemas de intrusión independientes. Esta diferencia es fundamental para el resultado de la velocidad de respuesta en PC con placas independientes que se muestra en una interfaz en la solicitud y no con módulos de interferencia de radios en un solo PC con esta y salida de información.

El solicitante alega que su dispositivo incluye una interfaz gráfica para coordinar ataques simultáneos. No obstante, D4 describe la coordinación de módulos de interferencia mediante un sistema centralizado conectado a un conmutador de red. La diferencia alegada corresponde a un aspecto de presentación o interfaz de usuario, que no afecta la esencia técnica de la invención ni introduce novedad frente al estado de la técnica. De igual manera, cabe mencionar que dicha característica no se menciona en el capítulo reivindicatorio. Es así como, en relación al quinto argumento, se tiene que el mismo no es de recibo por parte de esta Oficina, por lo mismo tales argumentos son insuficientes para otorgar las reivindicaciones 1 y 2.

Los argumentos del solicitante se basan en diferencias de implementación, ajustes de diseño o interpretaciones funcionales que no desvirtúan la anticipación realizada por D4. Conforme al artículo 16 de la Decisión 486, la invención no es nueva porque sus características esenciales ya están comprendidas en el estado de la técnica. En consecuencia, se mantiene la objeción de falta de novedad y se ratifica la negación de la solicitud.

Que de acuerdo con la modificación presentada por el solicitante en el escrito radicado bajo el N° NC2022/0007161 el 4 de diciembre de 2025 y teniendo en cuenta el objeto de la

Ref. Expediente N° NC2022/0007161

solicitud, se modifica el título de la invención el cual quedará de la siguiente manera: “DISPOSITIVO PARA LA INTRUSIÓN DE SEÑALES DE COMUNICACIÓN Y PARA LA INTRUSIÓN A SEÑALES DE GEOLOCALIZACIÓN DE DRONES”.

Con fundamento en las anteriores consideraciones, la Directora de Nuevas Creaciones (E),

RESUELVE

ARTÍCULO 1: Denegar la patente de modelo de utilidad para la creación titulada:

“DISPOSITIVO PARA LA INTRUSIÓN DE SEÑALES DE COMUNICACIÓN Y PARA LA INTRUSIÓN A SEÑALES DE GEOLOCALIZACIÓN DE DRONES”

ARTÍCULO 2: Notificar el contenido de la presente resolución a CENTRO DE INVESTIGACION Y DESARROLLO TECNOLÓGICO DE LA INDUSTRIA ELECTRO ELECTRONICA Y TIC CIDEI, advirtiéndole que contra ella procede el recurso de apelación ante la Superintendente Delegada para la Propiedad Industrial, el cual podrá ser interpuesto en el momento de la notificación o dentro de los diez (10) días hábiles siguientes a ella.

NOTIFÍQUESE Y CÚMPLASE

Dada en Bogotá D.C., el 30 de abril de 2026

LA DIRECTORA DE NUEVAS CREACIONES (E),



Sandra Isabel Calderon Rodriguez