

REPÚBLICA DE COLOMBIA
SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO

Oficio N° 18710 de 14 de noviembre de 2023

Ref. Expediente N° NC2021/0000053

Señores
YOUTRANSACTOR

TÍTULO DE LA SOLICITUD: “MÉTODO PARA PROTEGER UN TERMINAL DE PAGO”
NUMERO DE SOLICITUD INTERNACIONAL: PCT/EP2019/067471
FECHA DE PRESENTACIÓN INTERNACIONAL: 28 de junio de 2019.
PRIORIDAD: 29/06/2018, FR (FRANCIA), 1855990

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. Objeto de la invención

El problema planteado consiste en la necesidad de suministrar una solución de pago bancario menos costosa, al tiempo de ofrecer un nivel de seguridad por lo menos equivalente a las soluciones actuales, que permita proteger las claves criptográficas y brindar servicios de cifrado, descifrado, de autenticación y de firma electrónica para todo tipo de aplicaciones.

Para resolver dicho problema técnico, la solicitud en estudio proporciona un método para proteger un terminal de pago, en particular mediante tarjeta bancaria. La presente invención también se refiere a un terminal de pago seguro, especialmente mediante tarjeta bancaria.

2. Reivindicaciones estudiadas

El presente estudio se basa en el capítulo reivindicatorio presentado el 6 de enero de 2021.

3. No es una invención

En consideración con lo establecido en el literal e) del artículo 15 de la Decisión 486 de 2000 de la Comisión de la Comunidad Andina:

“No se consideran invenciones:

(...) e) los programas de ordenadores o el soporte lógico, como tales; y, (...)”

Debido a lo anterior, esta oficina determina que el objeto de la reivindicación 15 no se consideran como una invención, toda vez que, se refiere exclusivamente a un producto de programa informático.

Lo anterior se argumenta dado que la reivindicación independiente 15 recita: *“Un producto de programa informático que comprende instrucciones de código para la ejecución de un método (100) para proteger un terminal de pago (1) de acuerdo con cualquiera de las reivindicaciones 1 a 13 cuando se ejecuta este programa por un procesador.”*

Oficio N° 18710 de 14 de noviembre de 2023

Ref. Expediente N° NC2021/0000053

Sobre esta cláusula es posible detallar que ésta se refiere unica y exclusivamente a un programa de computadora y por lo tanto, no puede ser aceptada para estudio.

4. De la solicitud de patente

4.1. Reivindicaciones

Teniendo en cuenta lo establecido en el artículo 30 de la Decisión 486 de 2000 de la Comisión de la Comunidad Andina:

"Las reivindicaciones definirán la materia que se desea proteger mediante la patente. Deben ser claras y concisas y estar enteramente sustentadas por la descripción. (...)"

Esta oficina informa que, la reivindicación independiente 14 no es concisa porque repiten la materia reclamada en la reivindicación independiente 1 y solo se diferencian en el dispositivo al cual se está enfocando, específicamente en este caso *"Un terminal de pago seguro"*. En consecuencia, todas ellas son confusas y presentan el mismo alcance, por lo cual el capítulo carece de concisión. Se sugiere agrupar dichas alternativas teniendo en cuenta que exista una razonable generalización y que cada una de dichas alternativas tenga soporte en la descripción que permita una diferenciación real entre categorías.

En consecuencia, es necesario que allegue las aclaraciones o modificaciones correspondientes para dar cumplimiento a lo establecido en el citado artículo.

5. Determinación del Estado de la Técnica

La fecha para determinar el estado de la técnica es el 29 de junio de 2018, que corresponde a la fecha de presentación de la solicitud de prioridad.

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

Ítem	Documento	Título	Fecha de publicación
D1	EP0965902	"Secure data processor with cryptography and tamper detection"	22 de diciembre de 1999

D1¹ divulga un chip de Unidad de Procesamiento Seguro (SPU), un microprocesador diseñado especialmente para el procesamiento seguro de datos. Al integrar claves, motores de cifrado/descifrado y algoritmos en la SPU, todo el proceso de seguridad se vuelve portátil y se distribuye fácilmente a través de fronteras físicas. La invención se basa en la orquestación de tres sistemas interrelacionados: (i) detectores, que alertan a la SPU de la existencia y ayudan a caracterizar la naturaleza de un ataque a la seguridad; (ii) filtros, que correlacionan los datos de los distintos detectores, sopesando la gravedad del ataque frente al riesgo para la integridad de la SPU, tanto para sus datos secretos como para el propio diseño; y (iii) respuestas, que son contramedidas, calculadas por los filtros como las más apropiadas según las circunstancias, para hacer frente al ataque o ataques presentes. La presente invención, con amplia capacidad en los tres detectores, filtros y respuestas, permite un gran grado de flexibilidad para programar un nivel apropiado de seguridad/política en una aplicación basada en SPU (Resumen).

¹ <https://patentimages.storage.googleapis.com/83/ba/6a/a331143dcf3981/EP0965902A2.pdf>

Oficio N° 18710 de 14 de noviembre de 2023

Ref. Expediente N° NC2021/0000053

6. 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.

6.1. 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 (NC2021/0000053 del 6 de enero de 2021) refiere a: *“Un método (100) para proteger un terminal de pago (1), comprendiendo dicho terminal de pago (1). (...)”*. A continuación, se presenta la tabla comparativa entre el objeto reivindicado y los documentos encontrados en el estado de la técnica:

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

CARACTERÍSTICAS ESENCIALES	D1
Un método (100) para proteger un terminal de pago (1), comprendiendo dicho terminal de pago (1).	Procesador de datos seguro con criptografía y detección de manipulación (Título).
Una clave (MK) de cifrado de datos a la que se accede por cifrado de datos para asegurar.	(...) Estos circuitos integrados pueden almacenar por sí mismos información confidencial interna, como claves y/o algoritmos propietarios para cifrar y descifrar esa información, así como implementar el "motor" de cifrado/descifrado (...) (Párr. 0003).
Un módulo (120) de vigilancia de por lo menos un parámetro físico del terminal que comprende un medio de medición de dicho parámetro físico.	El Registro de Estado (11) es el depósito de todas las señales del detector de hardware dispuestas a través del dispositivo para detectar varios intentos de violación de la seguridad. Los detectores pueden incluir un fotodetector (16), un detector de temperatura (17), un detector de capa de metalización (18) y cualquier detector adicional (19) (representado en forma fantasma), por ejemplo: detectores de alto/bajo voltaje, detectores de vibración, detectores de arena (...) (Párr. 0029).
Un microcontrolador (10).	(...) microcontrolador CTRL (25) (...) (Párr. 0023).
Una unidad de contador de microcontrolador.	(...) El reloj de tiempo real (5) se implementa a través de un contador de ondulación binario que es controlado a través de RTCLK (29) por un cristal de cuarzo (14) externo fuera del chip de 32,768 KHz junto con el circuito del oscilador (14) RTC (...) (Párr. 0024).
Un reloj (LSI), estando la unidad de contador subordinada a dicho reloj para incrementar a intervalos regulares un valor de contador de la unidad de contador.	El reloj de tiempo real (5) para la SPU sigue el estándar IEEE (1212), que especifica la arquitectura de control y registro de estado (...) (Párr. 0024).
Dicho método comprende las siguientes etapas: (E10a) medición de un parámetro físico por el medio de medición del dispositivo de vigilancia.	(...) Los detectores pueden incluir un fotodetector (16), un detector de temperatura (17), un detector de capa de metalización (18) y cualquier detector adicional (19) (representado en forma fantasma), por ejemplo: detectores de alto/bajo voltaje, detectores de vibración, detectores de arena (...) (Párr. 0029).
(E10b) comparación del valor medido con un valor umbral predeterminado, correspondiente a un ataque físico a dicho terminal por parte del dispositivo de vigilancia.	(...) En una realización, el umbral para este interruptor es cuando VDD (22) excede 1, 2 veces VBAT (21). Si la batería externa está agotada, VBAT (21) es efectivamente cero y PWRGD 27 sube tan pronto como se enciende VDD (22) (...) (Párr. 0033).

Oficio N° 18710 de 14 de noviembre de 2023

Ref. Expediente N° NC2021/0000053

(E11) supresión del acceso a la clave (MK) de cifrado de datos por parte del microprocesador (10) si se cumple una de las siguientes condiciones.	(...) Si llega el momento de ejecutar la rutina de inversión de claves (802), el diagrama de flujo (800) se bifurca al bloque (808), lo que provoca que se deshabilite todo acceso a las claves (...) (Párr. 0066).
Por lo menos un valor de parámetros físicos es significativo de un ataque físico a dicho terminal; el valor de contador es mayor que un valor umbral predefinido; (E13) reinicio de la unidad de contador por el dispositivo de vigilancia; y en el que las etapas de medición (E10a), de comparación (E10b) y de reinicio (E13) se ejecutan periódicamente.	El Registro de Estado (11) es el depósito de todas las señales del detector de hardware dispuestas a través del dispositivo para detectar varios intentos de violación de la seguridad. Los detectores pueden incluir un fotodetector (16), un detector de temperatura (17), un detector de capa de metalización (18) y cualquier detector adicional (19) (representado en forma fantasma), por ejemplo: detectores de alto/bajo voltaje, detectores de vibración, detectores de arena (...) (Párr. 0029).

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

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

- Reivindicación 2: Normalmente, la SPU recibe "mensajes" en forma cifrada. El motor criptográfico (por ejemplo, DES Engine 6) utiliza claves, por ejemplo, "claves de sesión" específicas para una transacción de aplicación particular o "sesión". Por tanto, el motor criptográfico se utiliza para cifrar o descifrar los mensajes, o realizar otras operaciones criptográficas como es bien conocido en la técnica. Además de proporcionar una transferencia segura de mensajes, la SPU también proporciona una transferencia segura de claves. Al tener, o incluso generar una "clave maestra" internamente (utilizando cualquiera de las técnicas de generación de claves conocidas para algoritmos de claves públicas o secretas), la SPU puede recibir claves de sesión en forma cifrada y, tratándolas como mensajes, descifrarlas. con el motor criptográfico utilizando la clave maestra. Por el contrario, la SPU puede cifrar y enviar mensajes de forma segura. La clave maestra, las claves de sesión descifradas y otra información confidencial (por ejemplo, los algoritmos de cifrado/descifrado) se almacenan en una memoria regrabable segura en la SPU, como se describe a continuación (Párr. 0031).

- Reivindicación 3: (...) generar una "clave maestra" internamente (utilizando cualquiera de las técnicas de generación de claves conocidas para algoritmos de claves públicas o secretas), la SPU puede recibir claves de sesión en forma cifrada y, tratándolas como mensajes, descifrarlas. con el motor criptográfico utilizando la clave maestra. Por el contrario, la SPU puede cifrar y enviar mensajes de forma segura. La clave maestra, las claves de sesión descifradas y otra información confidencial (por ejemplo, los algoritmos de cifrado/descifrado) se almacenan en una memoria regrabable segura en la SPU, como se describe a continuación (Párr. 0031). (...) dicho usuario puede intentar operaciones simples, como intentar pasar el reloj o restablecer el dispositivo en varias etapas operativas, un usuario podría esperar interferir con los informes o la medición de uso. Además, también en el contexto de medición de información, al intentar sobrescribir la RAM 8, después de una compra grande, con el contenido de la misma RAM 8, anterior a la compra, un usuario podría esperar borrar los rastros de dicha transacción (...) (Párr. 0140). (...) Además, también en el contexto de medición de información, al intentar sobrescribir la RAM 8, después de una compra grande, con el contenido de la misma RAM 8, anterior a la compra, un usuario podría esperar borrar los rastros de dicha transacción (Párr. 0139). (...) Además, a veces es deseable destruir cierta información confidencial (por ejemplo, las claves) y preservar otra información confidencial (por ejemplo, datos históricos, como información contable utilizada en transacciones financieras) al detectarse una intrusión (Párr. 003). (...) La información secreta será

Oficio N° 18710 de 14 de noviembre de 2023

Ref. Expediente N° NC2021/0000053

destruida si se corta la alimentación de la SPU. Por otro lado, si la información secreta se coloca en la memoria no volátil, un atacante puede eliminar la SPU y, a su gusto y por medios convencionales, examinar la información en la memoria no volátil (Párr. 0063).

- Reivindicación 4: (...) un ejemplo de detector y medio de destrucción es un fotodetector conectado a un circuito de conmutación que corta la energía a las celdas de memoria dentro de un circuito integrado seguro al detectar luz. Cuando se apaga la alimentación, se perderá el contenido de las celdas de memoria, que pueden contener información confidencial. La teoría detrás de este mecanismo de seguridad es que el fotodetector quedará expuesto a la luz sólo cuando la carcasa del circuito integrado se rompa, intencionadamente o por accidente (...) (Párr. 0005).

- Reivindicación 5: (...) El otro terminal del multiplexor (742) está conectado a una señal externa (típicamente asíncrona). El dispositivo (748) genera una señal de reloj en la línea (752) que controla el multiplexor (742) de manera que la señal asíncrona externa en la línea (758) se acopla al flip-flop D (744) sólo en el momento t1. El dispositivo (748) también genera una señal de reloj en la línea (754) que controla la memoria intermedia 754 de manera que la señal de salida del flip-flop D (744) pasa a través de la memoria intermedia 746 sólo en el momento t3. Como resultado, la señal en la línea (756) está sincronizada (Párr. 0048).

- Reivindicación 6: Como se describió anteriormente, la señal DLY_PWRGD (26) se puede utilizar como reinicio. Sin embargo, si el contador PWRUP (102) se enciende en el estado incorrecto, puede afectar la operación de reinicio del resto del dispositivo. La máquina de estado en el contador PWRUP (102) podría encenderse en un estado de reinicio continuo debido a los requisitos duales de encender la punta sin reinicio y retrasar la parada de la sincronización CTTL (34) al apagarse. Para superar este problema, se proporciona un circuito analógico separado VccPUD (104), con entradas SET_PWUP (110) y CLR_PWUP (111), que configuran y borran respectivamente la salida VCCPWUP (107). El circuito VccPUD (104) también monitorea VDD (22) de manera que VCCPWUP (107) también borrará si VDD (22) cae por debajo de aproximadamente 2V. En esta realización, el VDD (22) es suministrado por el circuito de conmutación de energía 101 a través del VREF 115 (Párr. 0037). (...) La información secreta será destruida si se corta la alimentación de la SPU. Por otro lado, si la información secreta se coloca en la memoria no volátil, un atacante puede eliminar la SPU y, a su gusto y por medios convencionales, examinar la información en la memoria no volátil (Párr. 0063).

- Reivindicación 7: Cuando se aplica una señal externa, que generalmente es asíncrona, al terminal de entrada (732) del biestable (722), su estado (alto o bajo) se retiene en el biestable (722) sólo en el flanco ascendente del primer pulso de reloj. Este estado se mantiene igual hasta el flanco ascendente del segundo pulso de reloj. Como resultado, la señal de salida en el terminal (726) del flip-flop (722) permanece en el mismo estado desde el flanco ascendente del primer pulso de reloj hasta el flanco ascendente del segundo pulso de reloj, independientemente del estado de la señal de entrada entre los dos. bordes ascendentes (Párr. 0045). La señal PWRGD (27), al no originarse en el bus de datos interno 10, representaría un riesgo de seguridad dentro del circuito dentro del Silicon Firewall (20), si no se trata. Sin embargo, a diferencia de otras señales que pasan a través del Silicon Firewall (20), el PWRGD (27) se usa para iniciar el reloj del sistema (2), como se analiza a continuación, y por lo tanto no puede ser condicionado y sincronizado por el Silicon Firewall (20) de la manera en que se tratan esas otras señales. Por lo tanto, el circuito de conmutación de energía (101) condiciona la señal PWRGD (27) mediante un filtro de paso bajo, que actúa como un "devorador de fallas" para evitar cualquier cambio rápido en la señal PWRGD (27) resultante y darle un ancho de banda suficientemente estrecho como para admitir la señal PWRGD (27). circuitos internos (Párr. 0034).

Oficio N° 18710 de 14 de noviembre de 2023

Ref. Expediente N° NC2021/0000053

- Reivindicación 10: (...) Por tanto, el circuito de conmutación de alimentación (101) acondiciona la señal PWRGD (27) mediante un filtro de paso bajo, que actúa como un "devorador de fallas" para impedir cualquier cambio rápido en la señal PWRGD (27) resultante y darle un ancho de banda suficientemente estrecho como para admitir los circuitos internos (Párr. 0034). (...) La información secreta será destruida si se corta la alimentación de la SPU. Por otro lado, si la información secreta se coloca en la memoria no volátil, un atacante puede eliminar la SPU y, a su gusto y por medios convencionales, examinar la información en la memoria no volátil (Párr. 0063).

- Reivindicación 11: El Registro de Estado (11) es el depósito de todas las señales del detector de hardware dispuestas a través del dispositivo para detectar varios intentos de violación de la seguridad. Los detectores pueden incluir un fotodetector (16), un detector de temperatura (17), un detector de capa de metalización (18) y cualquier detector adicional (19) (representado en forma fantasma), por ejemplo: detectores de alto/bajo voltaje, detectores de vibración, detectores de arena. Cada uno de estos detectores puede transmitir uno o más bits de información que, en una realización, se almacenan en el Registro de Estado (11). El Registro de Estado (11) también puede almacenar señales generadas internamente, tales como la señal ROLLOVER (34) del Reloj de Tiempo Real (5) y el bit de RAM y Tiempo Válido (VRT), utilizado para verificar la integridad de la información almacenada en el Bloque de RAM (8) y el contador de tiempo en el Reloj de Tiempo Real (5) (Párr. 0029).

- Reivindicación 12: (...) como una estructura resistente a la manipulación dispuesta en un patrón que cubriría partes de la SPU, pero expondría otras de modo que el grabado de la estructura resistente a la manipulación destruye las partes expuestas. Por lo tanto, la SPU no sería fácilmente desmontada ni sometida a ingeniería inversa, porque la estructura resistente a manipulaciones ocultaría los circuitos activos y la eliminación de la estructura resistente a manipulaciones destruiría los circuitos activos. Este recubrimiento físico actuaría como un complemento natural del detector de capa de metalización (FIGS. 11-13) (Párr. 0068).

- Reivindicación 13: El proceso de filtrado programable es el núcleo de PDPS; sin él, uno simplemente tiene respuestas programadas e indiscriminadas a diversos ataques. Con referencia a la FIG. 19, este proceso en sí consta de dos etapas: (i) correlacionar las señales producidas por los diversos detectores para determinar los ataques involucrados (FIGS. 19(a), 19(b), 19(c)); y (ii) en función de los ataques involucrados, seleccionar una respuesta adecuada (FIGS. 19(d), 19(e), 19(f)). Por supuesto, hay factores operativos involucrados en ambas etapas de este proceso. Estos factores pueden ser estáticos e intrínsecamente relacionados con el tipo de aplicación, la arquitectura de la SPU, etc., o pueden variar dinámicamente y estar relacionados, por ejemplo, con: (i) el historial previo o la frecuencia de las señales y respuestas detectadas, o todos los eventos; (ii) el estado actual de la APE; (iii) la etapa o modalidad actual de la solicitud; (iv) el daño potencial que puede representar un determinado ataque; o (v) combinaciones de factores o detectores, por ejemplo, provenientes de un conjunto dado, que ocurren en un orden particular o que ocurren dentro de un período de tiempo fijo.

Las reivindicaciones dependientes 2 a 7 y 10 a 13 tampoco cumplen con el requisito de novedad.

Adicionalmente, los apartes de D1 mostrados en la tabla 1, sugieren las características técnicas reclamadas para las características del terminal de la reivindicación 14, por lo tanto, dicha reivindicación tampoco cumple con el requisito de novedad toda vez que su diferencia solo se centra en el cambio de dispositivo. Adicionalmente, por la falta de concisión que le ha sido advertido previamente.

Oficio N° 18710 de 14 de noviembre de 2023

Ref. Expediente N° NC2021/0000053

7. Conclusión

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

Ítem	Documento	Reivindicaciones afectadas	Requisito que afecta
D1	EP0965902	2 a 7 y 10 a 13 y 14	Novedad

En cumplimiento del artículo 45 de la Decisión 486 de 2000, se le indica que debe dar respuesta dentro del término de sesenta (60) días contados a partir de la fecha de notificación de la presente comunicación. En caso de no dar respuesta al presente requerimiento, o si a pesar de la respuesta subsistieran los impedimentos para la concesión, se denegará la patente.

Si como respuesta a este requerimiento, el solicitante modifica el capítulo reivindicatorio, deberá observar las instrucciones contenidas en el numeral 1.2.2.1.1., del Capítulo Primero del Título X de la Circular Única de esta Superintendencia. De igual forma, deberá tener presente que de conformidad con el literal a) del numeral 1.2.2.5.1. de la norma ibidem, será necesario acreditar el pago de la tasa por concepto de modificación a solicitudes en trámites, de conformidad con el valor establecido en la resolución de tasas vigentes.

Notifíquese el presente oficio conforme a lo dispuesto en el numeral 6.2 del Capítulo Sexto del Título I de la Circular Única, informándoles que contra el mismo no procede recurso alguno en actuación administrativa.



Edna Marcela Ramirez Orozco
DIRECTORA DE NUEVAS CREACIONES

Oficio N° 18710 de 14 de noviembre de 2023

Ref. Expediente N° NC2021/0000053

INFORME DE BÚSQUEDA
EXAMEN DE PATENTABILIDAD

Solicitud No.		Examen de patentabilidad							
NC2021/0000053		1°	X	2°		3°		Revoca	
Solicitud Internacional No.		Fecha solicitud internacional: (DD/MM/AÑO)							
PCT/EP2019/067471		28 de junio de 2019							
Fecha de determinación estado de la técnica (DD/MM/AÑO)				Prioridad		Presentación			
29/06/2018				X					
Solicitante									
YOUTRANSACTOR									
Reivindicaciones que no son objeto de búsqueda por:									
Art. 14	-	Art. 15	15	Art. 20	-	Art. 25 (Falta de unidad de invención)		-	
CRITERIOS DE BÚSQUEDA									
Reivindicaciones objeto de búsqueda				1 a 7, 10 a 13 y 14					
Palabras clave utilizadas				Secure, processor, data, cryptography, tamper, detection, clock, controller, destroy, erase, voltaile.					
Clasificaciones utilizadas para la búsqueda				CIP:	G06F 21/55, G06F 21/86, G07F 19/00				
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	95035010	07/10/1996	-	-			A		
WO	EP0965902	22/12/1999	1 a 7, 10 a 13 y 14	Todo el documento			X		
	FR2871905	23/12/2005	-	-			A		
	US2017017943	19/01/2017	-	-			A		
	Jiménez-Naharro, R., Gómez-Galán, J. A., Sánchez-Raya, M., Gómez-Bravo, F., & Pedro-Carrasco, M.	01/01/2013	-	-			A		
Patbase	US2019026724	24/01/2019	-	-			A		
⁽¹⁾ Cita completa literatura no patente (LNP) Apellido, A. A. (Fecha). Título del artículo. Nombre de la revista. Volumen(Número), pp-pp. O Apellido, A. A. (Fecha). Título del artículo. Nombre de la revista. Recuperado de http://xxxxxxx.		Jiménez-Naharro, R., Gómez-Galán, J. A., Sánchez-Raya, M., Gómez-Bravo, F., & Pedro-Carrasco, M. (2013). Design and implementation of a new real-time frequency sensor used as hardware countermeasure. Sensors, 13(9), 11709-11727.							
⁽²⁾ Categorías de documentos citados									
“A” Documento que define el estado general de la técnica no considerado como particularmente relevante.					“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.				
“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					“X” Documento particularmente relevante; la invención reivindicada no puede considerarse nueva o que implique una actividad inventiva por referencia al documento aisladamente considerado.				



Oficio N° 18710 de 14 de noviembre de 2023

Ref. Expediente N° NC2021/0000053

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.	“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: (20/10/2023)	

