

REPÚBLICA DE COLOMBIA
SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO

Oficio N° 6275 de 29 de mayo de 2020

Ref. Expediente N° NC2018/0010785

Señor(a)
SHOKESU S.L.

TÍTULO DE LA SOLICITUD: “SISTEMA DE MONITOREO Y EXTRACCIÓN DE INFORMACIONES PÚBLICAS DE USUARIOS REGISTRADOS EN REDES SOCIALES, ALOJADAS EN SERVIDORES Y NUBES DE DATOS DE REDES SOCIALES”

NÚMERO DE SOLICITUD INTERNACIONAL: PCT/ES2017/070125

FECHA DE PRESENTACIÓN INTERNACIONAL: 7 de marzo de 2017.

PRIORIDAD(ES): ES, P201630267, 7 de marzo de 2016.

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

De acuerdo con lo establecido en el numeral 1.2.2.2 del Capítulo Primero del Título X de la Circular Única para efectos del examen de patentabilidad, cuando la solicitud contenga más de diez (10) reivindicaciones y no se haya pagado la tasa complementaria, sólo se estudiarán las cubiertas por la tasa pagada al momento de realizar el examen de patentabilidad consagrado en el artículo 45 de la Decisión 486.

Por lo tanto, se estudiarán las reivindicaciones 1 a 9 del radicado N° NC2018/0010785 del 8 de octubre de 2018.

El problema planteado en esta solicitud consiste en la necesidad de monitorear y extraer de datos públicos alojados en servidores y nubes de datos de redes sociales y correspondientes a usuarios registrados en estas redes sociales.

Para resolver este problema técnico, la solicitud en estudio proporciona un método y un sistema de monitoreo y extracción de informaciones publicadas de usuarios registrados en redes sociales que comprende transmitir periódicamente a las API de redes sociales de forma que cada mensaje de consulta comprende al menos una identificación de una cuenta de usuario asignada a una credencial de acceso a la API de la red social y se envía sólo cuando la credencial de acceso comprende una clave de estado disponible y después de un tiempo transcurrido desde que la credencial de acceso ha sido utilizada por última vez para la transmisión de un mensaje de consulta, siendo el número de identificaciones de cuentas de usuario contenido en cada mensaje de consulta menor que un número máximo de peticiones de información efectuadas con una credencial de acceso admitido en un intervalo de tiempo determinado por la API de la red social.

2. De la solicitud de patente

2.1. Título



Oficio N° 6275 de 29 de mayo de 2020

Ref. Expediente N° NC2018/0010785

El nombre de la invención de que se trata en el artículo 27 literal d) de la Decisión 486 deberá reflejar el objeto y el campo industrial con el cual se relaciona la misma y ser concordante con la materia descrita y las reivindicaciones de la solicitud. El nombre no podrá referirse a nombres personales, marcas de productos o nombres de fantasía.

El solicitante en el escrito radicado bajo el N° NC2018/0010785 el 8 de octubre de 2018, tituló la invención como: “SISTEMA DE MONITOREO Y EXTRACCIÓN DE INFORMACIONES PÚBLICAS DE USUARIOS REGISTRADOS EN REDES SOCIALES, ALOJADAS EN SERVIDORES Y NUBES DE DATOS DE REDES SOCIALES”. Este título no se relaciona con el objeto de la solicitud contenido en la descripción y las reivindicaciones, por lo cual se sugiere el título siguiente: “MÉTODO Y SISTEMA DE MONITOREO Y EXTRACCIÓN DE INFORMACIONES PÚBLICAS DE USUARIOS REGISTRADOS EN REDES SOCIALES, ALOJADAS EN SERVIDORES Y NUBES DE DATOS DE REDES SOCIALES”.

2.2. Reivindicaciones (Art. 30 Decisión 486)

- Se recomienda revisar la dependencia de la reivindicación 9 que corresponde con un método puesto que esta depende de la reivindicación 8 que se refiere a un sistema y realizar la aclaración o modificación correspondiente.

3. Determinación del Estado de la Técnica

La fecha para determinar el estado de la técnica es el 7 de marzo de 2016 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	US20120303712	“Aggregation system”	29 de noviembre de 2012

El documento D1¹ divulga un sistema de agregación que incluye una computadora y hardware de red que conecta la computadora a una red. La computadora está programada para que el sistema de agregación presente una interfaz que se presente respectivamente a uno o más usuarios y que reciba información de dicho uno o más usuarios, analice la entrada para producir una agregación, permita ejecutar reglas definidas por el usuario que incluyen una capacidad para iniciar un proceso de alerta de modo que se envíe una comunicación correspondiente a la agregación a un destinatario y la agregue como salida (Resumen).

4. Examen de Patentabilidad (Art. 14 Decisión 486)

4.1. Novedad (Art. 16 Decisión 486)

La reivindicación 1 consiste en: “*Un método de monitoreo y extracción de informaciones publicadas de usuarios registrados en redes sociales alojadas en servidores y nubes de datos de redes sociales que comprende (...)*” (Radicado N° NC2018/0010785 del 8 de octubre de 2018).

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

¹<https://patents.google.com/patent/US20120303712A1/en?q=US2012303712>

Oficio N° 6275 de 29 de mayo de 2020

Ref. Expediente N° NC2018/0010785

Características esenciales	D1
Transmitir mensajes de consulta que comprenden credenciales de acceso a un API de cada red social, e identificaciones de cuentas de usuario de usuarios registrados en las redes públicas, a las direcciones URL de las redes sociales para obtener datos de las informaciones publicadas por los usuarios monitorizados, recibir las informaciones publicadas y guardarlas en una base de datos de informaciones.	(...) La aplicación cliente (7) utiliza las capacidades de comunicación subyacentes (por ejemplo, hardware de red, controladores de red y API de red proporcionada por el sistema operativo) del sistema de usuario (7) para comunicarse tanto con el sistema de servidor maestro (4) como con cualquiera de los sistemas de servidor de terceros (6n). El sistema de servidor maestro (4) almacena información persistente para permitir el acceso a los sistemas de servidor de terceros (6n). Esta información puede incluir la ubicación del servidor y las credenciales de autenticación de usuario necesarias para acceder a cualquier sistema de servidor de terceros (6n). La aplicación cliente (7) es capaz de recuperar esta información persistente (por ejemplo, direcciones de red de servidores de terceros y credenciales de usuario para ese servicio) del servidor maestro (4) para acceder directamente a los sistemas de servidores de terceros, incluidos los procedimientos de autenticación necesarios (Párr. 0113). La información agregada puede almacenarse en una base de datos y / o presentarse de una manera discernible para el ser humano (por ejemplo, pantalla, sonido, etc.) en el sistema informático del usuario (2) (Párr. 0187).
Caracterizado porque los mensajes de consulta (1) se transmiten periódicamente a las API (7) de las redes sociales (8) de forma que cada mensaje de consulta (1) comprende al menos una identificación de una cuenta de usuario (4) registrada en la red social (8), asignada a una credencial de acceso (2) a la API (7) de una red social (8).	(...) En el bloque (72), el Applet compara periódicamente los metadatos del lado del servidor con los datos subyacentes del proveedor de servicios externo mediante una operación de diferencia estándar entre las ID de correo electrónico y / u otros metadatos disponibles (...) (Párr. 0038). (...) Esta información puede incluir la ubicación del servidor y las credenciales de autenticación de usuario necesarias para acceder a cualquier sistema de servidor de terceros (6n) (...) (Párr. 0113).
Cada mensaje de consulta (1) se envía sólo cuando la credencial de acceso (2) comprende una clave de estado disponible (9a).	(...) La aplicación del lado del cliente se puede adaptar para recibir las credenciales y para comunicar las partes respectivas de las credenciales para obtener acceso a cada uno de una pluralidad de sistemas de servidor de terceros (6), y para permitir que el sistema informático del usuario (2) agregue información del tercero sistemas de servidor (6) (Párr. 0186).
Después de un tiempo transcurrido desde que la credencial de acceso (2) ha sido utilizada por última vez para la transmisión de un mensaje de consulta (1), calculado desde una fecha y hora de último acceso identificada por una clave de último acceso (2a).	(...) El Applet verifica periódicamente si hay nuevos mensajes en un servicio de terceros buscando mensajes con marcas de tiempo más nuevas que la última marca de tiempo de verificación de mensaje nuevo. Esto ocurre cada n minutos y los pasos a continuación se ejecutan una vez por carpeta en cada servicio. (...) En el bloque 81, si se encuentran nuevos mensajes, los metadatos (Desde, Asunto, Fecha de envío, Indicador de archivos adjuntos, estado de lectura, etc.) se analizan para cada uno de los mensajes nuevos (...) (Párr. 0139).
Cada mensaje de consulta (1) se marca con un código de completación (6) identificativo de una fecha y hora de completación de la transmisión del mensaje de consulta (1).	(...) En el bloque (80), el Applet recupera la lista de mensajes de correo del servicio de terceros, analiza el mensaje y busca cualquier mensaje con una marca de tiempo más reciente que el último mensaje almacenado en el servidor (...) (Párr. 0139).
El código de completación (6) del mensaje de consulta (1) transmitido se asigna a la credencial de acceso (2) como la clave de último acceso (2a).	(...) El Applet carga estos nuevos metadatos al Servidor a través de llamadas de servicio web SOAP. El servidor almacena estos nuevos datos en la tabla de metadatos del correo electrónico en la base de datos (...) (Párr. 0139).
Después de un periodo de tiempo predeterminado (t), calculado desde la fecha y hora de último acceso identificada por la clave de último acceso (2a),	Ahora se llama la atención sobre el proceso de verificación de mensajes nuevos (FIG. 15). En el bloque (79), el Applet verifica periódicamente si hay nuevos mensajes en un servicio de terceros buscando mensajes con marcas de tiempo más nuevas que la última marca de tiempo de verificación de mensaje nuevo. Esto ocurre cada

Oficio N° 6275 de 29 de mayo de 2020

Ref. Expediente N° NC2018/0010785

se vuelve a enviar un mensaje de consulta (1) con la credencial de acceso (2) a la que se ha asignado el código de último acceso (2a).	n minutos y los pasos a continuación se ejecutan una vez por carpeta en cada servicio (...) (Párr. 0079).
El número de identificaciones de cuentas de usuario (4) contenido en cada mensaje de consulta (1) es menor que un número máximo de peticiones de información efectuadas con una credencial de acceso (2) admitido en un intervalo de tiempo determinado por la API (7) de la red social (8) sin entrar en un periodo de bloqueo temporal.	Para procesar el correo electrónico agregado desde múltiples sitios, en una realización, el sistema del servidor maestro podría acceder a Yahoo, MSN, Gmail, MySpace y otros sitios de servicios web. Esto se puede hacer recuperando el contenido de URL del lado del servidor para acceder a los sitios ilustrativos mencionados anteriormente. Sin embargo, es concebible que estas empresas puedan bloquear dicho acceso, por ejemplo, bloqueando las direcciones IP finitas del sistema del servidor maestro, lo que podría paralizar o cerrar la agregación (es decir, las solicitudes de realización del lado del servidor se originarían en un IP del lado del servidor único o limitado) Para abordar el problema de bloqueo de IP, en otra realización, el sistema del servidor maestro puede tener un applet firmado que se descargará automáticamente al sistema informático del usuario. (...) Las solicitudes que se originen en el lado del applet contendrían la dirección IP del usuario final (los proveedores no bloquearían una dirección IP de usuario final) (Párr. 0103).

De acuerdo con la tabla anterior, las características esenciales del método de la reivindicación 1 habían sido divulgadas previamente en el documento D1, por lo tanto, la materia reivindicada no es nueva.

La reivindicación 7 consiste en: “*Sistema de monitoreo y extracción de informaciones públicas de usuarios registrados de redes sociales, alojadas en servidores y nubes de datos de redes sociales que comprende (...)*” (Radicado N° NC2018/0010785 del 8 de octubre de 2018).

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

Características esenciales	D1
Un dispositivo transmisor (11) para transmitir mensajes de consulta (1) a cuentas de usuario seleccionadas empleando credenciales de acceso (2) a APIs (7) de cada red social (8).	En una forma interesante de redactar una realización, el sistema informático del usuario (2) puede recibir, del sistema del servidor maestro (4), credenciales respectivas para acceder a cada uno de una pluralidad de sistemas de servidores de terceros y luego implementar las credenciales de acceso recibidas para producir una agregación de información. (...) En consecuencia, la información transmitida entre la aplicación del lado del cliente y la aplicación del lado del servidor puede permitir agregar las comunicaciones en una presentación en el sistema informático del usuario (Párr. 0189).
Un dispositivo receptor de informaciones (12) para recibir y extraer datos de las informaciones publicadas en las cuentas de usuario seleccionadas a las que se ha accedido a través de cada API (7) mediante la transmisión de un mensaje de consulta (1).	Para la búsqueda de empleo y los componentes de compra, el sistema del servidor maestro puede recuperar las páginas apropiadas en función de la consulta de búsqueda de todas las cuentas de usuario. Para los componentes de noticias, el sistema del servidor maestro puede recuperar las páginas apropiadas en función de la categoría y / o fuente de todas las cuentas de usuario (Párr. 0091). Para cualquiera de los contenidos recuperados, el sistema del servidor maestro puede "leer con anticipación" y recuperar y almacenar en caché el contenido en la memoria local en base a la solicitud anticipada de recuperación para reducir el tiempo entre la solicitud y la representación del contenido (Párr. 0092).
Un dispositivo de almacenamiento (13) para almacenar los datos publicados clasificados de cuenta de usuario monitorizada.	La información agregada puede almacenarse en una base de datos y / o presentarse de una manera discernible para el ser humano (por ejemplo, pantalla, sonido, etc.) en el sistema informático del usuario (2) (Párr. 0187).

Oficio N° 6275 de 29 de mayo de 2020

Ref. Expediente N° NC2018/0010785

Caracterizado porque comprende un dispositivo seleccionador de credenciales (21), diseñado para seleccionar credenciales de acceso (2) disponibles contenidas en una base de datos de credenciales (10) en la que a cada credencial de acceso (2) le están asignadas a una clave de último acceso (2a) y una clave de estado (9), siendo la clave de último acceso (2a) identificativa de una fecha y hora de último acceso en la que la credencial de acceso (2) ha sido utilizada por última vez en un mensaje de consulta (1) transmitido, y siendo la clave de estado (9) una clave de estado disponible (9a) o una clave de estado ocupado (9b), donde cada credencial de acceso (2) disponible comprende una clave de estado disponible (9a) y una clave de último acceso (2a) identificativa de un periodo de tiempo transcurrido con una fecha y hora inicial anterior a la fecha y hora inicial de un periodo de tiempo transcurrido predeterminado (t).	(...) El sistema de servidor maestro (4) almacena información persistente para permitir el acceso a los sistemas de servidor de terceros (6n). Esta información puede incluir la ubicación del servidor y las credenciales de autenticación de usuario necesarias para acceder a cualquier sistema de servidor de terceros (6n). La aplicación cliente (7) es capaz de recuperar esta información persistente (por ejemplo, direcciones de red de servidores de terceros y credenciales de usuario para ese servicio) del servidor maestro (4) para acceder directamente a los sistemas de servidores de terceros, incluidos los procedimientos de autenticación necesarios (Párr. 0113). (...) La aplicación del lado del cliente se puede adaptar para recibir las credenciales y para comunicar las partes respectivas de las credenciales para obtener acceso a cada uno de una pluralidad de sistemas de servidor de terceros (6), y para permitir que el sistema informático del usuario (2) agregue información del tercero sistemas de servidor (6) (Párr. 0186). Ahora se llama la atención sobre el proceso de verificación de mensajes nuevos (FIG. 15). En el bloque (79), el Applet verifica periódicamente si hay nuevos mensajes en un servicio de terceros buscando mensajes con marcas de tiempo más nuevas que la última marca de tiempo de verificación de mensaje nuevo. Esto ocurre cada n minutos y los pasos a continuación se ejecutan una vez por carpeta en cada servicio (...) (Párr. 0079).
Un dispositivo formador de mensajes de consulta (15) para formar mensajes de consulta (1) dirigidas a cada API (7), comprendiendo cada mensaje de consulta (1) al menos una identificación de cuenta de usuario (4) registrada en la red social, asignada a una credencial de acceso (2) a la API (7) de dicha red social (8), siendo el número de identificaciones de cuentas de usuario (4) en cada mensaje de consulta (1) menor que un número máximo de peticiones de información efectuadas con una misma credencial de acceso (2) admitido en un intervalo de tiempo determinado por la API (7) sin entrar en un periodo de bloqueo temporal.	Para procesar el correo electrónico agregado desde múltiples sitios, en una realización, el sistema del servidor maestro podría acceder a Yahoo, MSN, Gmail, MySpace y otros sitios de servicios web. Esto se puede hacer recuperando el contenido de URL del lado del servidor para acceder a los sitios ilustrativos mencionados anteriormente. Sin embargo, es concebible que estas empresas puedan bloquear dicho acceso, por ejemplo, bloqueando las direcciones IP finitas del sistema del servidor maestro, lo que podría paralizar o cerrar la agregación (es decir, las solicitudes de realización del lado del servidor se originarían en un IP del lado del servidor único o limitado) Para abordar el problema de bloqueo de IP, en otra realización, el sistema del servidor maestro puede tener un applet firmado que se descargará automáticamente al sistema informático del usuario. (...) Las solicitudes que se originen en el lado del applet contendrían la dirección IP del usuario final (los proveedores no bloquearían una dirección IP de usuario final) (Párr. 0103).
Un dispositivo detector (16) diseñado para detectar la fecha y hora en la que un mensaje de consulta (1) ha sido transmitido y para marcar cada mensaje de consulta (1) transmitido con un código de completación (6) identificativo de la fecha y hora de completación de la	(...) El Applet verifica periódicamente si hay nuevos mensajes en un servicio de terceros buscando mensajes con marcas de tiempo más nuevas que la última marca de tiempo de verificación de mensaje nuevo. Esto ocurre cada n minutos y los pasos a continuación se ejecutan una vez por carpeta en cada servicio. (...) En el bloque 81, si se encuentran nuevos mensajes, los metadatos (Desde, Asunto, Fecha de envío, Indicador de archivos adjuntos, estado de lectura, etc.) se analizan para cada uno de los mensajes nuevos (...) (Párr. 0139).

Oficio N° 6275 de 29 de mayo de 2020

Ref. Expediente N° NC2018/0010785

transmisión del mensaje de consulta (1).	
Un dispositivo asignador (17) diseñado para asignar el código de completación (6) como fecha y hora de último acceso a la credencial de acceso (2) contenida en cada mensaje de consulta (1) transmitido.	(....) En el bloque (80), el Applet recupera la lista de mensajes de correo del servicio de terceros, analiza el mensaje y busca cualquier mensaje con una marca de tiempo más reciente que el último mensaje almacenado en el servidor (...) (Párr. 0139).
Un dispositivo cambiador de claves de estado (22), diseñado para cambiar la clave de estado disponible (9a) de cada una de las credenciales de acceso (2) seleccionadas a la clave de estado ocupado (9b), y para cambiar la clave de estado ocupado (9b) asignada a la credencial de acceso (2) contenida en cada mensaje de consulta (1) transmitido en una clave de estado disponible (9a).	(...) La aplicación cliente (7) es capaz de recuperar esta información persistente (por ejemplo, direcciones de red de servidores de terceros y credenciales de usuario para ese servicio) del servidor maestro (4) para acceder directamente a los sistemas de servidores de terceros, incluidos los procedimientos de autenticación necesarios (Párr. 0113). En una forma interesante de redactar una realización, el sistema informático del usuario (2) puede recibir, del sistema del servidor maestro (4), credenciales respectivas para acceder a cada uno de una pluralidad de sistemas de servidores de terceros y luego implementar las credenciales de acceso recibidas para producir una agregación de información. (...) En consecuencia, la información transmitida entre la aplicación del lado del cliente y la aplicación del lado del servidor puede permitir agregar las comunicaciones en una presentación en el sistema informático del usuario (Párr. 0189).
Un dispositivo iterador (19) diseñado para ordenar al dispositivo seleccionador la selección de nuevas credenciales de acceso (2) disponibles contenidas en la base de credenciales (10) para iniciar sucesivamente la formación de nuevos mensajes de consulta (1).	(...) La aplicación del lado del cliente se puede adaptar para recibir las credenciales y para comunicar las partes respectivas de las credenciales para obtener acceso a cada uno de una pluralidad de sistemas de servidor de terceros (6), y para permitir que el sistema informático del usuario (2) agregue información del tercero sistemas de servidor (6) (Párr. 0186).

De acuerdo con la tabla anterior, las características esenciales del sistema de la reivindicación 7 habían sido divulgadas previamente en el documento D1, por lo tanto, la materia reivindicada no es nueva.

5. Conclusión con respecto a novedad y/o nivel inventivo

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

Ítem	Documento	Reivindicaciones afectadas	Requisito que afecta
D1	US20120303712	1 y 7	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: i) el capítulo reivindicatorio, ii) la descripción de la invención a proteger, iii) o presenta un nuevo 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 y la Dirección de Nuevas Creaciones seguirá el procedimiento descrito en el numeral 1.2.2.5.1.

Oficio N° 6275 de 29 de mayo de 2020

Ref. Expediente N° NC2018/0010785

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° 6275 de 29 de mayo de 2020

Ref. Expediente N° NC2018/0010785

INFORME DE BÚSQUEDA
EXAMEN DE PATENTABILIDAD

Solicitud No.		Examen de patentabilidad							
NC2018/0010785		1°	X	2°		3°		Revoca	
Solicitud Internacional No.		Fecha solicitud internacional: (DD/MM/AÑO)							
PCT/ES2017/070125		7 de marzo de 2017							
Fecha de determinación estado de la técnica (DD/MM/AÑO)				Prioridad		Presentación			
07/03/2016				X					
Solicitante									
SHOKESU S.L.									
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 9
Palabras clave utilizadas	Monitor and Extract Information, Retrieve Information, Social Network, User Profile, Query, Request, Access Credentials, API, User Account, URL, Cloud, Server, Database, Status, Lock.
Clasificaciones utilizadas para la búsqueda	CIP: G06F 21/62

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	15161482	28/12/2015	-	-	A
EP	US20120303712	29/11/2012	1 y 7	1 Párr. 0113, Párr. 0187, Párr. 0038, Párr. 0186, Párr. 0139, Párr. 0079, Párr. 0103. 7 Párr. 0189, Párr. 0091, Párr. 0092, Párr. 0187, Párr. 0113, Párr. 0186, Párr. 0079, Párr. 0103, Párr. 0139.	X
	US20140245411	28/08/2014	-	-	A
	US20111179161	21/07/2011	-	-	A
Patbase	US2011113096	12/05/2011	-	-	A
⁽¹⁾ Cita completa literatura no patente (LNP)					
Apellido, A. A. (Fecha). Título del artículo. Nombre de la revista. Volumen(Número), pp-pp.					
O					
Apellido, A. A. (Fecha). Título del artículo. Nombre de la revista. Recuperado de http://xxxxxxx.					
⁽²⁾ Categorías de documentos citados					
“A” Documento que define el estado general de la técnica no considerado como particularmente relevante.			“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.					

Oficio N° 6275 de 29 de mayo de 2020

Ref. Expediente N° NC2018/0010785

“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.	“X” Documento particularmente relevante; la invención reivindicada no puede considerarse nueva o que implique una actividad inventiva por referencia al documento aisladamente considerado. “Y” Documento particularmente relevante; la invención reivindicada no puede considerarse que implique una actividad inventiva cuando el documento se asocia a otro u otros documentos de la misma naturaleza, cuya combinación resulta evidente para un experto en la materia.
Fecha del reporte de búsqueda: (05/05/2020)	
Examinador: CARLOS EDUARDO GUEVARA NICHROY	