

REPÚBLICA DE COLOMBIA
SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO

Oficio N° 15807 de 28 de septiembre de 2023

Ref. Expediente N° NC2020/0005673

Señores
IDEMIA IDENTITY & SECURITY FRANCE

TÍTULO DE LA SOLICITUD: “MÉTODO PARA LA AUTENTICACIÓN FUERTE DE UN INDIVIDUO”

PRIORIDAD: 24/05/2019, FR (FRANCIA), 1905521

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 simple, confiable y segura que sea completamente respetuosa de la privacidad para la autenticación de un individuo, en particular para fines de recuperación.

Para resolver dicho problema técnico, la solicitud en estudio proporciona un método para autenticación fuerte de un individuo implementada mediante un servidor y un dispositivo cliente conectado (...) (Resumen).

2. Reivindicaciones estudiadas

El presente estudio se basa en el capítulo reivindicatorio presentado el 7 de mayo de 2020.

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 16 no se consideran como una invención, toda vez que, se refiere a un programa de ordenador.

Lo anterior se sustenta dado que la reivindicación dependiente 16 recita: *“Un producto de programa informático que comprende instrucciones de código para la ejecución de un método de acuerdo con una de las reivindicaciones 1 a 14 para la autenticación fuerte de un individuo tras lo cual dicho programa se ejecuta en una computadora”*.

Sobre esta cláusula es posible detallar que se refieren exclusivamente a un “programa informático”, es decir, se refiere a un programa de ordenador.

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:

Oficio N° 15807 de 28 de septiembre de 2023

Ref. Expediente N° NC2020/0005673

"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, las reivindicaciones independientes 1 y 15 hacen referencia a los dibujos, según la expresión *"como se ilustra en la imagen captada"*. Se sugiere eliminar la referencia al dibujo o imagen e indicar las características que se quieren reclamar de manera específica.

Esta oficina informa que, la reivindicación independiente 15 no es concisa porque repiten la materia reclamada en la reivindicación independiente 1 y solo se diferencian en el dispositivo, el cual está enfocado en cada uno de los productos que hacen parte de la invención en su conjunto. 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.

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 24 de mayo de 2019, que corresponde a la fecha de presentación de la solicitud de prioridad.

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

Ítem	Documento	Título	Fecha de publicación
D1	US2018176017	"Digital Identity System"	21 de julio de 2018
D2	WO2016166478	"Methods of generating and verifying a security key of a virtual monetary unit"	21 junio de 2018

D1¹ divulga un método de un sistema de identidad digital que genera un token compartido para autenticar a un portador ante un validador, en el que un almacén de datos del sistema de identidad digital contiene una pluralidad de atributos del portador, comprendiendo el método implementar por parte del sistema de identidad digital los siguientes pasos: recibir en el sistema de identidad digital desde un portador una solicitud de token de intercambio electrónico, en donde la solicitud de token identifica al menos uno de los atributos del portador en el almacén de datos seleccionado para compartir con un validador; en respuesta a la solicitud de token electrónico, generar un token compartido, que es exclusivo de esa solicitud, para que el portador lo presente a un validador; asociar con el token de intercambio único en el sistema de identidad digital el al menos un atributo de portador identificado; y emitir al portador la ficha de participación única; y en el que la presentación posterior del token compartido único al sistema de identificación digital por parte de un validador hace que el al menos un atributo de portador asociado con el token compartido se ponga a disposición del validador mediante el sistema de identidad digital (Resumen).

D2² divulga un método de generación de una clave de seguridad de una unidad monetaria virtual de un proyecto, adquirida por un usuario de un dispositivo cliente conectado por una red a una plataforma que comprende medios de almacenamiento de datos almacenar una base de datos de unidades monetarias virtuales, cada una de ellas al menos

¹ <https://patentimages.storage.googleapis.com/23/d2/2a/8894be21095b04/US20180176017A1.pdf>

² <https://patentimages.storage.googleapis.com/21/4d/07/73ee7069ca3fa1/WO2016166478A1.pdf>

Oficio N° 15807 de 28 de septiembre de 2023

Ref. Expediente N° NC2020/0005673

asociada con: un identificador único de la unidad monetaria, un identificador único del proyecto de dicha unidad monetaria virtual y un identificador único de dicho usuario que ha adquirido dicha unidad monetaria virtual (...) (Resumen).

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. 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 (NC2020/0005673 del 7 de mayo de 2020) refiere a: *“Método para autenticación fuerte de un individuo implementada mediante un servidor (2) y un dispositivo cliente conectado (3). (...)”*. 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 esenciales con las del estado de la técnica.

CARACTERÍSTICAS ESENCIALES	D1	D2
Método para autenticación fuerte de un individuo implementada mediante un servidor (2) y un dispositivo cliente conectado (3).	Sistema de identidad digital (Título).	Métodos para generar y verificar una clave de seguridad de una unidad monetaria virtual (Título).
El dispositivo cliente (3) que tiene un dato biométrico candidato del individuo.	En otras realizaciones, se puede utilizar otro tipo de datos biométricos (distintos o adicionales al selfie), como la imagen de una huella dactilar o una plantilla biométrica (por ejemplo, LBP) derivada de ella (Párr. 0616).	No menciona.
Y una imagen captada de un documento de identidad (1) que representa al menos una fotografía de dicho individuo.	(...) La primera aplicación móvil sirve para escanear elementos de datos de un documento de identidad y transmitirlos al servicio central (14) (Párr. 0249). En el estado de la técnica es común que las aplicaciones de dispositivos móviles permitan escanear a partir de las imágenes captadas por la cámara del dispositivo móvil.	No menciona.
Y un dato del lector óptico visible en dicho documento de identidad (1).	La aplicación de autenticación uPass presenta una credencial apropiada (30) a un lector uPass (54) en la aplicación (52) que luego la envía al servicio de autorización (14b) para su autenticación. Si esta operación de autenticación tiene éxito, la aplicación de lectura de uPass (52) recibirá acceso a uno o más perfiles de uPass y el usuario podrá entonces confirmar su identidad basándose en elementos de datos del perfil que	No menciona.



Oficio N° 15807 de 28 de septiembre de 2023

Ref. Expediente N° NC2020/0005673

	ahora puede ver, como por ejemplo una foto (Párr. 0445).	
Y el servidor (2) tiene una huella criptográfica de una primera concatenación de dicho dato del lector óptico de dicho documento de identidad (1) y de un primer dato aleatorio, la denominada huella criptográfica.	No menciona.	(...) (a) generar una primera porción de clave de seguridad representativa del proyecto, comprendiendo dicha primera porción de clave una primera huella digital criptográfica de al menos el identificador único de dicho proyecto, y una pluralidad de caracteres aleatorios insertados en posiciones predeterminadas en dicha primera huella (...) (Reiv. 1). (...) siendo la primera huella criptográfica una huella criptográfica de una concatenación del identificador y código de dicho proyecto (Pág. 7, líneas 16 a 19).
En donde el método se caracteriza porque comprende la implementación mediante los medios de procesamiento de datos (21, 31) del servidor (2) y/o del dispositivo cliente (3) de las etapas de;	una interfaz informática; un procesador configurado para ejecutar una aplicación de identidad digital, en donde la aplicación de identidad digital está configurada cuando se ejecuta en el procesador para realizar operaciones (Párr. 0043).	La plataforma 2 es típicamente un servidor que comprende medios de procesamiento de datos 21 (por ejemplo, un procesador) y medios de almacenamiento de memoria 22, por ejemplo un disco duro) (Pág. 5, líneas 16 a 18).
(b) extraer, mediante el análisis de dicha imagen captada de dicho documento de identidad (1).	(...) La primera aplicación móvil sirve para escanear elementos de datos de un documento de identidad y transmitirlos al servicio central (14) (Párr. 0249).	No menciona.
Una información candidata representativa de la apariencia de dicha fotografía como se ilustra en la imagen captada.	(...) las fotografías incrustadas se comparan con la fotografía de confirmación del solicitante de registro en el servicio de reconocimiento facial (40) para garantizar un parecido visual. (Párr. 0419).	
Dicho dato del lector óptico como se ilustra en la imagen captada.	(...) El lector uPass (54) solicita credenciales para autenticación (...) (Párr. 00513).	No menciona.
c) calcular un primer dato decodificado mediante la aplicación de un proceso de decodificación a dicha información candidata representativa de la apariencia de dicha fotografía y a un primer dato codificado, de tal manera que el primer dato decodificado coincide con el primer dato aleatorio si dicha información candidata representativa de la apariencia de dicha fotografía coincide con una información de referencia representativa de la apariencia de dicha fotografía.	(...) un código respectivo único para esa entidad (portador/validador), en donde el método puede comprender: generar un código compuesto único combinando el código del portador con el código del validador, en donde ninguno de los códigos puede derivarse únicamente del código compuesto (...) (Párr. 0032). (...) las fotografías incrustadas se comparan con la fotografía de confirmación del solicitante de registro en el servicio de reconocimiento facial (40) para garantizar un parecido visual. (Párr. 0419).	un módulo para generar una primera porción de clave de seguridad representativa del proyecto, comprendiendo dicha primera porción de clave una primera huella digital criptográfica de al menos el identificador único de dicho proyecto, y una pluralidad de caracteres aleatorios insertados en posiciones predeterminadas; en dicha primera impresión (Pág. 3, líneas 25 a 28).
Verificar que: una huella criptográfica de una primera	No menciona.	(...) cada una de estas huellas generadas se compara con la

Oficio N° 15807 de 28 de septiembre de 2023

Ref. Expediente N° NC2020/0005673

concatenación del dato extraído del lector óptico y del dato decodificado coincida con dicha primera huella criptográfica en posesión del servidor (2).		primera parte de la clave introducida a la que se le eliminan los diferentes caracteres aleatorios que se habían añadido (para encontrar la unicidad de la primera huella). Si hay una coincidencia, entonces la primera parte de la clave es válida y ahora sabemos a qué proyecto referirnos, lo que reduce significativamente el tiempo de búsqueda para verificar el resto de la clave (...) (Pág. 9, líneas 3 a 9). (...) siendo la primera huella criptográfica una huella criptográfica de una concatenación del identificador y código de dicho proyecto (Pág. 7, líneas 16 a 19).
Y el dato biométrico de referencia y el dato biométrico candidato del individuo coincidan.	El al menos un identificador de validador puede comprender: al menos una plantilla biométrica del validador, y/o al menos un secreto conocido sólo por el validador, y/o una imagen del validador (Párr. 0025). (...) las fotografías incrustadas se comparan con la fotografía de confirmación del solicitante de registro en el servicio de reconocimiento facial (40) para garantizar un parecido visual. (Párr. 0419).	No menciona.

D1 es considerado como el estado de la técnica más cercano a la invención definida en la reivindicación 1, ya que divulga un sistema de identidad digital (Título).

La diferencia entre la invención definida entre la reivindicación 1 y el método divulgado en D1, consiste en que la solicitud en estudio incluye una huella criptográfica de una primera concatenación y verificar que dicha huella criptográfica coincida con la huella criptográfica almacenada en el servidor.

El efecto que se logra al incluir una huella criptográfica de una primera concatenación y verificar que dicha huella criptográfica coincida con la huella criptográfica almacenada en el servidor es que calcular una diferencia de acuerdo con que una métrica dada sea menor que un umbral para determinar la veracidad de la información.

Por lo tanto, el problema técnico objetivo que pretende resolver esta invención se puede formular así: ¿cómo modificar el método divulgado en D1 para calcular una diferencia de acuerdo con que una métrica dada sea menor que un umbral para determinar la veracidad de la información?

Sin embargo, el incluir una huella criptográfica de una primera concatenación y verificar que dicha huella criptográfica coincida con la huella criptográfica almacenada en el servidor para calcular una diferencia de acuerdo con que una métrica dada sea menor que un umbral para determinar la veracidad de la información, ya está divulgado en D2 que se refiere a: (...) (a) generar una primera porción de clave de seguridad representativa del proyecto, comprendiendo dicha primera porción de clave una primera



Oficio N° **15807** de **28 de septiembre de 2023**

Ref. Expediente N° NC2020/0005673

huella digital criptográfica de al menos el identificador único de dicho proyecto, y una pluralidad de caracteres aleatorios insertados en posiciones predeterminadas en dicha primera huella (...) (Reiv. 1). (...) cada una de estas huellas generadas se compara con la primera parte de la clave introducida a la que se le eliminan los diferentes caracteres aleatorios que se habían añadido (para encontrar la unicidad de la primera huella). Si hay una coincidencia, entonces la primera parte de la clave es válida y ahora sabemos a qué proyecto referirnos, lo que reduce significativamente el tiempo de búsqueda para verificar el resto de la clave (...) (Pág. 9, líneas 3 a 9). (...) siendo la primera huella criptográfica una huella criptográfica de una concatenación del identificador y código de dicho proyecto (Pág. 7, líneas 16 a 19).

En consecuencia, la persona normalmente versada en la materia al verse enfrentada al problema técnico objetivo de calcular una diferencia de acuerdo con que una métrica dada sea menor que un umbral para determinar la veracidad de la información estaría motivada a incluir una huella criptográfica de una primera concatenación y verificar que dicha huella criptográfica coincida con la huella criptográfica almacenada en el servidor del D2 en el método 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: En otras realizaciones, se puede utilizar otro tipo de datos biométricos (distintos o adicionales al selfie), como la imagen de una huella dactilar o una plantilla biométrica (por ejemplo, LBP) derivada de ella (Párr. 0616). (...) las fotografías incrustadas se comparan con la fotografía de confirmación del solicitante de registro en el servicio de reconocimiento facial (40) para garantizar un parecido visual. (Párr. 0419).

- Reivindicación 3: Un pasaporte electrónico (10) u otro documento de identidad (por ejemplo, permiso de conducir) se lee mediante un dispositivo móvil (12) (por ejemplo, a través de NFC) y los datos de registro se pasan al servicio uPass (14) de forma segura a través de Internet, como se describe más adelante. El servicio uPass almacena el registro de datos en uno o más perfiles que forman parte de una identidad digital (28) (Párr. 00254). En el estado de la técnica es común que los dispositivos móviles incluyan elementos para extraer datos biométricos.

- Reivindicación 6: (...) En otras realizaciones, se puede utilizar otro tipo de datos biométricos (distintos o adicionales al selfie), como la imagen de una huella dactilar o una plantilla biométrica (por ejemplo, LBP) derivada de ella (Párr. 0616). (...) La primera aplicación móvil sirve para escanear elementos de datos de un documento de identidad y transmitirlos al servicio central (14) (Párr. 0249). En el paso (S402), se extrae un conjunto de uno o más atributos {a*} del nuevo documento (202N) (permiso de conducir en este ejemplo), que se transmite al servidor de inscripción (14a) (S404) junto con la clave de usuario cifrada Dk(Uk), un identificador del uID del usuario que se comparará con el que se mantiene en el sistema 1 y la credencial actual del usuario c. En el paso (S406), el servidor de inscripción 14a compara los atributos recién capturados {a*} con los atributos {a} retenidos en el sistema en la medida en que dicha comparación sea posible (...) (Párr. 0138). En el estado de la técnica es común que las aplicaciones de dispositivos móviles permitan escanear a partir de las imágenes captadas por la cámara del dispositivo móvil.

- Reivindicación 8: El al menos un identificador de validador puede comprender: al menos una plantilla biométrica del validador, y/o al menos un secreto conocido sólo por el validador, y/o una imagen del validador (Párr. 0025). (...) las fotografías incrustadas se comparan con la fotografía de confirmación del solicitante de registro en el servicio de

Oficio N° 15807 de 28 de septiembre de 2023

Ref. Expediente N° NC2020/0005673

reconocimiento facial (40) para garantizar un parecido visual. (Párr. 0419). Un pasaporte electrónico (10) u otro documento de identidad (por ejemplo, permiso de conducir) se lee mediante un dispositivo móvil (12) (por ejemplo, a través de NFC) y los datos de registro se pasan al servicio uPass (14) de forma segura a través de Internet, como se describe más adelante. El servicio uPass almacena el registro de datos en uno o más perfiles que forman parte de una identidad digital (28) (Párr. 00254). En el estado de la técnica es común que los dispositivos móviles incluyan elementos para extraer datos biometricos.

- Reivindicación 12: (...) Se proporciona un mecanismo automatizado 67 para realizar un arbitraje de confianza oportuno entre usuarios mediante credenciales ofrecidas (por ejemplo, códigos QR). Cada componente del sistema se describirá ahora con más detalle a continuación (Párr. 0252).

- Reivindicación 17: También se proporciona un producto de programa informático que comprende código almacenado en un medio de almacenamiento legible por computadora configurado para implementar cualquier método o sistema descrito en el presente documento (Párr. 0222).

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

- Reivindicaciones 2, 3, 6, 8, 12: (...) (a) generar una primera porción de clave de seguridad representativa del proyecto, comprendiendo dicha primera porción de clave una primera huella digital criptográfica de al menos el identificador único de dicho proyecto, y una pluralidad de caracteres aleatorios insertados en posiciones predeterminadas en dicha primera huella (...) (Reiv. 1). (...) cada una de estas huellas generadas se compara con la primera parte de la clave introducida a la que se le eliminan los diferentes caracteres aleatorios que se habían añadido (para encontrar la unicidad de la primera huella). Si hay una coincidencia, entonces la primera parte de la clave es válida y ahora sabemos a qué proyecto referirnos, lo que reduce significativamente el tiempo de búsqueda para verificar el resto de la clave (...) (Pág. 9, líneas 3 a 9). (...) siendo la primera huella criptográfica una huella criptográfica de una concatenación del identificador y código de dicho proyecto (Pág. 7, líneas 16 a 19).

Las reivindicaciones dependientes 2, 3, 6, 8, 12 y 17 tampoco cumplen con el requisito de nivel inventivo.

Adicionalmente, los apartes de D1 y D2 mostrados en la tabla 1, anticipan las características técnicas reclamadas para las características de la unidad de autenticación fuerte, el servidor conectado y el dispositivo cliente que se reclama en la reivindicación 15, por lo tanto, dicha reivindicación tampoco cumple con el requisito de nivel inventivo toda vez que su diferencia solo se centra en la inclusión del método en el dispositivo.

7. Conclusión

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

Ítem	Documento	Reivindicaciones afectadas	Requisito que afecta
D1	US2018176017	1, 2, 3, 6, 8, 12, 15, y 17	Nivel inventivo
D2	WO2016166478	1, 2, 3, 6, 8, 12, 15, y 17	Nivel inventivo

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

Oficio N° 15807 de 28 de septiembre de 2023

Ref. Expediente N° NC2020/0005673

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° 15807 de 28 de septiembre de 2023

Ref. Expediente N° NC2020/0005673

INFORME DE BÚSQUEDA
EXAMEN DE PATENTABILIDAD

Solicitud No.		Examen de patentabilidad							
NC2020/0005673		1°	X	2°		3°		Revoca	
Fecha de determinación estado de la técnica (DD/MM/AÑO)				Prioridad		Presentación			
24/05/2019				X					
Solicitante									
IDEMIA IDENTITY & SECURITY FRANCE									
Reivindicaciones que no son objeto de búsqueda por:									
Art. 14	-	Art. 15	16	Art. 20	-	Art. 25 (Falta de unidad de invención)		-	
CRITERIOS DE BÚSQUEDA									
Reivindicaciones objeto de búsqueda				1 a 15 y 17					
Palabras clave utilizadas				Method, generat*, verif*, security, key, identification, digital, fingerprint, cryptographic, biometric, capture, image, smartphone.					
Clasificaciones utilizadas para la búsqueda				CIP:	G06F 21/31, G06F 21/32				
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	NC2022/0000102	17/01/2022	-	-				T	
EPO	WO2018/233487	27/12/2018	-	-				A	
	Shi, Y., & Jain, A. K	01/01/2019	-	-				A	
	Sutcu, Y., Li, Q., & Memon, N	01/09/2007	-	-				A	
Patbase	US2018176017	21/07/2018	1, 2, 3, 6, 8, 12, 15, y 17	Todo el documento				Y	
	WO2016166478	21/06/2018	1, 2, 3, 6, 8, 12, 15, y 17	Todo el documento				Y	
⁽¹⁾ Cita completa literatura no patente (LNP)		Shi, Y., & Jain, A. K. (2019). DocFace+: ID document to selfie matching. IEEE Transactions on Biometrics, Behavior, and Identity Science, 1(1), 56-67.							
Apellido, A. A. (Fecha). Título del artículo. Nombre de la revista. Volumen(Número), pp-pp.		Sutcu, Y., Li, Q., & Memon, N. (2007). Protecting biometric templates with sketch: Theory and practice. IEEE Transactions on Information Forensics and Security, 2(3), 503-512.							
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.									



Oficio N° 15807 de 28 de septiembre de 2023

Ref. Expediente N° NC2020/0005673

Fecha del reporte de búsqueda: (03/09/2023)

