

REPÚBLICA DE COLOMBIA
SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO

Oficio N° 9787 de 24 de junio de 2021

Ref. Expediente N° NC2019/0007656

Señor(a)
LLC MICROSOFT TECHNOLOGY LICENSING

TÍTULO DE LA SOLICITUD: **“SELLADO DE DATOS CON UN ENCLAVE DE SELLADO”**

NÚMERO DE SOLICITUD INTERNACIONAL: PCT/US2017/067455

FECHA DE PRESENTACIÓN INTERNACIONAL: 20 de diciembre de 2017.

PRIORIDAD(ES): 24/01/2017, US (ESTADOS UNIDOS DE AMÉRICA), 15/414,492

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 15 del radicado N° NC2019/0007656 del 16 de julio de 2019.

El problema planteado en esta solicitud consiste en la necesidad de suministrar un método y sistema de aislamiento de un enclave local confiable de código local no confiable fuera del aislamiento del enclave, habilitando la informática confiable remota.

Para resolver este problema técnico, la solicitud en estudio proporciona técnicas para sellar y desellar de manera segura datos de enclave a través de plataformas. Los datos de enclave de un enclave de origen alojado en una primera computadora pueden sellarse de manera segura en un enclave de sellado en una segunda computadora, y pueden además desellarse de manera segura para un enclave de destino en una tercera computadora.

2. De la solicitud de patente

2.1 Título

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° NC2019/0007656 el 16 de julio de 2019, tituló la invención como: “SELLADO DE DATOS CON UN ENCLAVE DE SELLADO”. Este título no se relaciona con el objeto de la solicitud contenido en la descripción y las



Oficio N° 9787 de 24 de junio de 2021

Ref. Expediente N° NC2019/0007656

modalidades descritas en las reivindicaciones, por lo cual se sugiere el título siguiente: “MÉTODO Y SISTEMA DE SELLADO DE DATOS CON UN ENCLAVE DE SELLADO”.

2.2 Reivindicaciones (Art. 30 Decisión 486)

- Se solicita corregir los errores de redacción de la siguiente frase: *“restringir el acceso de los datos de enclave enclaves con identidades autenticadas se permite de acuerdo con la lista permitida”* (reivs. 1 y 6).
- Se sugiere incluir entre paréntesis () los números de referencia de cada uno de los elementos que hacen parte de la invención de acuerdo con la numeración empleada en los dibujos, con el fin, de hacer más fácil la comprensión de la materia reivindicada.

3. Determinación del Estado de la Técnica

La fecha para determinar el estado de la técnica es el 24 de enero de 2017 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	US 2015/347768	“Policy-Based Trusted Inspection of Rights Managed Content”	03 de diciembre de 2015
D2	US 2015/304736	“Technologies For Hardening The Security Of Digital Information On Client Platforms”	22 de octubre de 2015
D3	US 2013/198853	“Method and apparatus to provide secure application execution”	01 de agosto de 2013

El documento D1¹ divulga un método ejecutado por al menos un procesador que comprende inicializar el primer y segundo enclaves seguros, cada uno de los cuales comprende un entorno de ejecución de software confiable que evita que el software que se ejecuta fuera del primer y segundo enclaves seguros tenga acceso a software y datos dentro del primer y segundo enclaves seguros (Pág. 1, Resumen).

El documento D2² divulga tecnologías para fortalecer la seguridad de la información digital en un dispositivo cliente (Pág. 1, Resumen).

El documento D3³ divulga una técnica para permitir una aplicación segura y la integridad de los datos dentro de un sistema informático. En una realización, se establecen uno o más enclaves seguros en los que se pueden almacenar y ejecutar una aplicación y datos (Pág. 1, Resumen).

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

4.1 Novedad (Art 16 Decisión 486)

¹https://worldwide.espacenet.com/publicationDetails/biblio?CC=US&NR=2015347768A1&KC=A1&FT=D&ND=3&date=20151203&DB=&locale=en_EP

²https://worldwide.espacenet.com/publicationDetails/biblio?II=0&ND=3&adjacent=true&locale=en_EP&FT=D&date=20151022&CC=US&NR=2015304736A1&KC=A1

³https://worldwide.espacenet.com/publicationDetails/biblio?CC=US&NR=2013198853A1&KC=A1&FT=D&ND=3&date=20130801&DB=&locale=en_EP

Oficio N° 9787 de 24 de junio de 2021

Ref. Expediente N° NC2019/0007656

La reivindicación 1 consiste en: “Un método para sellar datos de enclave, que comprende: (...)” (Radicado N° NC2019/0007656 del 16 de julio de 2019).

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

Características esenciales	D1	D2
Un método para sellar datos de enclave, que comprende: (...)	Un método ejecutado por al menos un procesador que comprende inicializar el primer y segundo enclaves seguros, cada uno de los cuales comprende un entorno de ejecución de software confiable que evita que el software que se ejecuta fuera del primer y segundo enclaves seguros tenga acceso a software y datos dentro del primer y segundo enclaves seguros (Pág. 1, Resumen).	En algunas realizaciones, el dispositivo cliente incluye un entorno de procesamiento seguro, como un enclave seguro, que puede usarse para proteger información digital en una plataforma cliente (Pág. 1, Resumen).
Enviar, a un enclave de origen alojado en una primera plataforma de enclave nativa, un primer reporte de afirmación de un enclave de sellado alojado en una segunda plataforma de enclave nativa.	A este respecto, el CPM (306) puede hacer que el nodo (101) envíe un reporte de enclave a un módulo de cotización como el módulo de cotización (307) (Pág. 5, Párr. 058). Las instrucciones CPM también pueden hacer que el nodo (101) selle el ID de la lista blanca en el enclave de memoria (304) (Pág. 8, Párr. 085).	En este sentido, CPM (306) puede hacer que el cliente (101) envíe un reporte de enclave a un módulo de cotización como el módulo de cotización (307) (Pág. 8, Párr. 089). Las instrucciones de CPM también pueden hacer que el cliente (101) selle el ID de la lista blanca en el enclave de memoria (304) (Pág. 10, Párr. 115).
Recibir una lista permitida y datos de enclave asociados del enclave de origen, en donde la lista permitida incluye una lista de una o más identidades de enclave permitidas para desellar los datos de enclave.	Después del aprovisionamiento, el nodo (101) puede autenticarse en el nodo (102) desellando los secretos dentro del enclave seguro (304) y enviando su ID de lista blanca al nodo (102), por ejemplo, en un mensaje firmado. El nodo (102) puede verificar la autenticidad del cliente verificando la firma aplicada al mensaje y comparando el ID de la lista blanca del cliente con los ID de la lista blanca de las plataformas aprobadas (Pág. 6, Párr. 068).	Después del aprovisionamiento, el cliente (101) puede autenticarse en el servidor (102) desellando los secretos dentro del enclave seguro (304) y enviando su ID de lista blanca al servidor (102), por ejemplo, en un mensaje firmado. El servidor (102) puede verificar la autenticidad del cliente verificando la firma aplicada al mensaje y comparando el ID de la lista blanca del cliente con los ID de la lista blanca de las plataformas aprobadas (Pág. 9, Párr. 098).
Almacenar de manera segura los datos de enclave y la lista permitida.	Las instrucciones SPM también pueden hacer que el nodo (102) genere un ID de lista blanca para el nodo (101), que puede almacenarse en asociación con la información recibida en la cotización del enclave. Por ejemplo, las instrucciones SPM pueden hacer que el nodo (102) almacene el ID de la lista blanca en la base de datos (314), en asociación con otra información recibida del nodo (101) (Pág. 7, Párr. 083).	Las instrucciones SPM también pueden hacer que el servidor (102) genere un ID de lista blanca para el cliente (101), que puede almacenarse en asociación con la información recibida en la cotización del enclave. Por ejemplo, las instrucciones SPM pueden hacer que el servidor (102) almacene el ID de la lista blanca en la base de datos (314), en asociación con otra información recibida del cliente (101) (Pág. 11, Párr. 113).
Restringir el acceso de los datos de enclave enclaves con identidades autenticadas se permite de acuerdo con la lista permitida.	El nodo (102) puede verificar la autenticidad del cliente verificando la firma aplicada al mensaje y comparando el ID de la lista blanca del cliente con los ID de la lista	El servidor (102) puede verificar la autenticidad del cliente verificando la firma aplicada al mensaje y comparando el ID de la lista blanca del cliente con los ID de la lista

Oficio N° 9787 de 24 de junio de 2021

Ref. Expediente N° NC2019/0007656

	blanca de las plataformas aprobadas. Debido a que el nodo (101) puede revelar los secretos dentro del enclave de memoria (304), el texto sin formato de dichos secretos puede protegerse de malware u otras entidades no autorizadas residentes en el cliente (101) (Pág. 6, Párr. 068).	blanca de las plataformas aprobadas. Debido a que el cliente (101) puede revelar los secretos dentro del enclave de memoria (304), el texto sin formato de dichos secretos puede protegerse de malware u otras entidades no autorizadas residentes en el cliente (101) (Pág. 9, Párr. 098).
--	--	---

De acuerdo con la tabla anterior, las características esenciales del método de la reivindicación 1 habían sido divulgadas previamente en los documentos D1 y D2, por lo tanto, la materia reivindicada no es nueva.

Asimismo, el documento D1 divulga las características de las reivindicaciones dependientes así:

- Reivindicación 2: A este respecto, el CPM (306) puede hacer que el nodo (101) envíe un reporte de enclave a un módulo de cotización como el módulo de cotización (307) (Pág. 5, Párr. 058). El nodo (101) y el nodo (102), respectivamente, incluyen plataformas de dispositivos (301), (308). Sin limitación, las plataformas de dispositivos (301), (308) pueden correlacionarse con uno o más tipos de dispositivos, como servidores, clientes, nodos de computación móvil, teléfonos inteligentes, tabletas, computadoras portátiles, netbooks y similares (Pág. 4, Párr. 043). El nodo (101) también puede incluir el módulo de cotización (307), que puede incluir instrucciones legibles por computadora que cuando se ejecutan (por ejemplo, por el procesador (302)) pueden hacer que el nodo (101) realice operaciones de verificación de informes de enclave y operaciones de generación de cotizaciones de enclave consistentes (Pág. 4, Párr. 052).
- Reivindicación 3: A este respecto, el CPM (306) puede hacer que el nodo (101) envíe un reporte de enclave a un módulo de cotización como el módulo de cotización (307) (Pág. 5, Párr. 058). El nodo (102) puede verificar la autenticidad del cliente verificando la firma aplicada al mensaje y comparando el ID de la lista blanca del cliente con los ID de la lista blanca de las plataformas aprobadas. Debido a que el nodo (101) puede revelar los secretos dentro del enclave de memoria (304), el texto sin formato de dichos secretos puede protegerse de malware u otras entidades no autorizadas residentes en el cliente (101) (Pág. 6, Párr. 068).
- Reivindicación 4: La capacidad de una parte remota para verificar que las medidas del enclave y los ajustes de la plataforma estén configurados como se espera se conoce como atestación. SGX utiliza dos credenciales relacionadas para la certificación: informes y cotizaciones. Se usa un informe para verificar la exactitud de los enclaves en la plataforma local, y se puede usar una cotización para reflejar la plataforma y el estado del enclave a entidades fuera de la plataforma (Pág. 3, Párr. 039). Las instrucciones CPM también pueden hacer que el nodo (101) selle el ID de la lista blanca en el enclave de memoria (304) (Pág. 8, Párr. 085). El bloque (745) incluye el segundo enclave seguro que descifra el contenido cifrado para producir contenido descifrado e inspecciona el contenido descifrado (Pág. 10, Párr. 114).
- Reivindicación 5: Las instrucciones CPM también pueden hacer que el nodo (101) selle el ID de la lista blanca en el enclave de memoria (304), por ejemplo, cifrando el ID de la lista blanca con la clave del enclave de la memoria del enclave (304) (Pág. 8, Párr. 085). Las instrucciones SPM también pueden hacer que el nodo (102)

Oficio N° 9787 de 24 de junio de 2021

Ref. Expediente N° NC2019/0007656

genere un ID de lista blanca para el nodo (101), que puede almacenarse en asociación con la información recibida en la cotización del enclave. Por ejemplo, las instrucciones SPM pueden hacer que el nodo (102) almacene el ID de la lista blanca en la base de datos (314), en asociación con otra información recibida del nodo (101) (Pág. 7, Párr. 083). El término "medio legible por máquina" o "medio de almacenamiento" deberá incluir, entre otros, memorias como memorias de estado sólido, discos ópticos y magnéticos, memoria de solo lectura (ROM), ROM programable (PROM), borrable PROM (EPROM), EPROM eléctricamente (EEPROM), una unidad de disco, un disquete, un disco compacto ROM (CD-ROM), un disco versátil digital (DVD), memoria flash (...) (Pág. 11, Párr. 119). El bloque (740) incluye el primer nodo seguro que comunica contenido cifrado al segundo enclave seguro en respuesta a la autenticación del segundo enclave seguro. El bloque (745) incluye el segundo enclave seguro que descifra el contenido cifrado para producir contenido descifrado e inspecciona el contenido descifrado (Pág. 10, Párr. 114).

Las reivindicaciones dependientes 2 a 5 tampoco cumplen con el requisito de novedad.

La reivindicación 6 consiste en: “Un sistema que comprende al menos un procesador y memoria que almacena (...)” (Radicado N° NC2019/0007656 del 16 de julio de 2019).

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

Características esenciales	D1	D2
Un sistema que comprende al menos un procesador y memoria que almacena en la misma instrucciones que, cuando son ejecutadas por el sistema, provocan al menos: (...)	El ejemplo 18 incluye un aparato que comprende: al menos una memoria; al menos un procesador, acoplado a la memoria, para realizar operaciones que comprenden (...) (Pág. 13, Párr. 150).	Otro ejemplo de la presente divulgación es un dispositivo cliente que incluye: un procesador; una memoria que tiene información digital cifrada almacenada en la misma, estando cifrada la información digital cifrada con al menos una clave de cifrado de información (Pág. 24, Párr. 265).
Enviar, a un enclave de origen alojado en una primera plataforma de enclave nativa, un primer reporte de afirmación de un enclave de sellado alojado en una segunda plataforma de enclave nativa.	A este respecto, el CPM (306) puede hacer que el nodo (101) envíe un reporte de enclave a un módulo de cotización como el módulo de cotización (307) (Pág. 5, Párr. 058). Las instrucciones CPM también pueden hacer que el nodo (101) selle el ID de la lista blanca en el enclave de memoria (304) (Pág. 8, Párr. 085).	En este sentido, CPM (306) puede hacer que el cliente (101) envíe un reporte de enclave a un módulo de cotización como el módulo de cotización (307) (Pág. 8, Párr. 089). Las instrucciones de CPM también pueden hacer que el cliente (101) selle el ID de la lista blanca en el enclave de memoria (304) (Pág. 10, Párr. 115).
Recibir una lista permitida y datos de enclave asociados del enclave de origen, en donde la lista permitida incluye una lista de una o más identidades de enclave permitidas para desellar los datos de enclave.	Después del aprovisionamiento, el nodo (101) puede autenticarse en el nodo (102) desellando los secretos dentro del enclave seguro (304) y enviando su ID de lista blanca al nodo (102), por ejemplo, en un mensaje firmado. El nodo (102) puede verificar la autenticidad del cliente verificando la firma aplicada al mensaje y comparando el ID de la lista blanca del cliente con los ID de la lista blanca de las plataformas aprobadas (Pág. 6, Párr. 068).	Después del aprovisionamiento, el cliente (101) puede autenticarse en el servidor (102) desellando los secretos dentro del enclave seguro (304) y enviando su ID de lista blanca al servidor (102), por ejemplo, en un mensaje firmado. El servidor (102) puede verificar la autenticidad del cliente verificando la firma aplicada al mensaje y comparando el ID de la lista blanca del cliente con los ID de la lista blanca de las plataformas aprobadas (Pág. 9, Párr. 098).
Almacenar de manera	Las instrucciones SPM también	Las instrucciones SPM también

Oficio N° 9787 de 24 de junio de 2021

Ref. Expediente N° NC2019/0007656

segura los datos de enclave y la lista permitida.	pueden hacer que el nodo (102) genere un ID de lista blanca para el nodo (101), que puede almacenarse en asociación con la información recibida en la cotización del enclave. Por ejemplo, las instrucciones SPM pueden hacer que el nodo (102) almacene el ID de la lista blanca en la base de datos (314), en asociación con otra información recibida del nodo (101) (Pág. 7, Párr. 083).	pueden hacer que el servidor (102) genere un ID de lista blanca para el cliente (101), que puede almacenarse en asociación con la información recibida en la cotización del enclave. Por ejemplo, las instrucciones SPM pueden hacer que el servidor (102) almacene el ID de la lista blanca en la base de datos (314), en asociación con otra información recibida del cliente (101) (Pág. 11, Párr. 113).
Restringir el acceso de los datos de enclave enclaves con identidades autenticadas se permite de acuerdo con la lista permitida.	El nodo (102) puede verificar la autenticidad del cliente verificando la firma aplicada al mensaje y comparando el ID de la lista blanca del cliente con los ID de la lista blanca de las plataformas aprobadas. Debido a que el nodo (101) puede revelar los secretos dentro del enclave de memoria (304), el texto sin formato de dichos secretos puede protegerse de malware u otras entidades no autorizadas residentes en el cliente (101) (Pág. 6, Párr. 068).	El servidor (102) puede verificar la autenticidad del cliente verificando la firma aplicada al mensaje y comparando el ID de la lista blanca del cliente con los ID de la lista blanca de las plataformas aprobadas. Debido a que el cliente (101) puede revelar los secretos dentro del enclave de memoria (304), el texto sin formato de dichos secretos puede protegerse de malware u otras entidades no autorizadas residentes en el cliente (101) (Pág. 9, Párr. 098).

De acuerdo con la tabla anterior, las características esenciales del sistema de la reivindicación 6 habían sido divulgadas previamente en los documentos D1 y D2, por lo tanto, la materia reivindicada no es nueva.

Asimismo, el documento D1 divulga las características de las reivindicaciones dependientes así:

- Reivindicación 7: A este respecto, el CPM (306) puede hacer que el nodo (101) envíe un reporte de enclave a un módulo de cotización como el módulo de cotización (307) (Pág. 5, Párr. 058). El nodo (101) y el nodo (102), respectivamente, incluyen plataformas de dispositivos (301), (308). Sin limitación, las plataformas de dispositivos (301), (308) pueden correlacionarse con uno o más tipos de dispositivos, como servidores, clientes, nodos de computación móvil, teléfonos inteligentes, tabletas, computadoras portátiles, netbooks y similares (Pág. 4, Párr. 043). El nodo (101) también puede incluir el módulo de cotización (307), que puede incluir instrucciones legibles por computadora que cuando se ejecutan (por ejemplo, por el procesador (302)) pueden hacer que el nodo (101) realice operaciones de verificación de informes de enclave y operaciones de generación de cotizaciones de enclave consistentes (Pág. 4, Párr. 052).
- Reivindicación 8: A este respecto, el CPM (306) puede hacer que el nodo (101) envíe un reporte de enclave a un módulo de cotización como el módulo de cotización (307) (Pág. 5, Párr. 058). El nodo (102) puede verificar la autenticidad del cliente verificando la firma aplicada al mensaje y comparando el ID de la lista blanca del cliente con los ID de la lista blanca de las plataformas aprobadas. Debido a que el nodo (101) puede revelar los secretos dentro del enclave de memoria (304), el texto sin formato de dichos secretos puede protegerse de malware u otras entidades no autorizadas residentes en el cliente (101) (Pág. 6, Párr. 068).

Oficio N° 9787 de 24 de junio de 2021

Ref. Expediente N° NC2019/0007656

- Reivindicación 9: La capacidad de una parte remota para verificar que las medidas del enclave y los ajustes de la plataforma estén configurados como se espera se conoce como atestación. SGX utiliza dos credenciales relacionadas para la certificación: informes y cotizaciones. Se usa un informe para verificar la exactitud de los enclaves en la plataforma local, y se puede usar una cotización para reflejar la plataforma y el estado del enclave a entidades fuera de la plataforma (Pág. 3, Párr. 039). Las instrucciones CPM también pueden hacer que el nodo (101) selle el ID de la lista blanca en el enclave de memoria (304) (Pág. 8, Párr. 085). El bloque (745) incluye el segundo enclave seguro que descifra el contenido cifrado para producir contenido descifrado e inspecciona el contenido descifrado (Pág. 10, Párr. 114).
- Reivindicación 10: Las instrucciones CPM también pueden hacer que el nodo (101) selle el ID de la lista blanca en el enclave de memoria (304), por ejemplo, cifrando el ID de la lista blanca con la clave del enclave de la memoria del enclave (304) (Pág. 8, Párr. 085). Las instrucciones SPM también pueden hacer que el nodo (102) genere un ID de lista blanca para el nodo (101), que puede almacenarse en asociación con la información recibida en la cotización del enclave. Por ejemplo, las instrucciones SPM pueden hacer que el nodo (102) almacene el ID de la lista blanca en la base de datos (314), en asociación con otra información recibida del nodo (101) (Pág. 7, Párr. 083). El término "medio legible por máquina" o "medio de almacenamiento" deberá incluir, entre otros, memorias como memorias de estado sólido, discos ópticos y magnéticos, memoria de solo lectura (ROM), ROM programable (PROM), borrable PROM (EPROM), EPROM eléctricamente (EEPROM), una unidad de disco, un disquete, un disco compacto ROM (CD-ROM), un disco versátil digital (DVD), memoria flash (...) (Pág. 11, Párr. 119). El bloque (740) incluye el primer nodo seguro que comunica contenido cifrado al segundo enclave seguro en respuesta a la autenticación del segundo enclave seguro. El bloque (745) incluye el segundo enclave seguro que descifra el contenido cifrado para producir contenido descifrado e inspecciona el contenido descifrado (Pág. 10, Párr. 114).

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

La reivindicación 11 consiste en: “*Un sistema que comprende al menos un procesador y memoria que almacena (...)*” (Radicado N° NC2019/0007656 del 16 de julio de 2019).

Tabla 3. Comparación de las características técnicas esenciales, con las del estado de la técnica

Características esenciales	D1	D2
Un sistema que comprende al menos un procesador y memoria que almacena en la misma instrucciones que, cuando son ejecutadas por el sistema, provocan al menos: (...)	El ejemplo 18 incluye un aparato que comprende: al menos una memoria; al menos un procesador, acoplado a la memoria, para realizar operaciones que comprenden (...) (Pág. 13, Párr. 150).	Otro ejemplo de la presente divulgación es un dispositivo cliente que incluye: un procesador; una memoria que tiene información digital cifrada almacenada en la misma, estando cifrada la información digital cifrada con al menos una clave de cifrado de información (Pág. 24, Párr. 265).
Recibir, en un enclave de origen alojado en una primera plataforma de enclave nativa, un primer reporte de afirmación de un enclave de sellado alojado en una segunda plataforma	A este respecto, el CPM (306) puede hacer que el nodo (101) envíe un reporte de enclave a un módulo de cotización como el módulo de cotización (307) (Pág. 5, Párr. 058).	En este sentido, CPM (306) puede hacer que el cliente (101) envíe un reporte de enclave a un módulo de cotización como el módulo de cotización (307) (Pág. 8, Párr. 089). Las instrucciones de CPM también

Oficio N° 9787 de 24 de junio de 2021

Ref. Expediente N° NC2019/0007656

de enclave nativa.	Las instrucciones CPM también pueden hacer que el nodo (101) selle el ID de la lista blanca en el enclave de memoria (304) (Pág. 8, Párr. 085).	pueden hacer que el cliente (101) selle el ID de la lista blanca en el enclave de memoria (304) (Pág. 10, Párr. 115).
Verificar la confianza en el enclave de sellado.	Por lo tanto, una realización puede tener un primer enclave seguro que reconoce el segundo enclave seguro como un enclave confiable (...) (Pág. 10, Párr. 113).	Si todas las operaciones de verificación se completan con éxito, SPM (312) puede determinar que el enclave de memoria (304) en el cliente (101) es válido y confiable (Pág. 9, Párr. 096).
Enviar una lista permitida y datos de enclave asociados hacia el enclave de sellado, en donde la lista permitida incluye una lista de una o más identidades de enclave permitidas para desellar los datos de enclave.	Después del aprovisionamiento, el nodo (101) puede autenticarse en el nodo (102) desellando los secretos dentro del enclave seguro (304) y enviando su ID de lista blanca al nodo (102), por ejemplo, en un mensaje firmado. El nodo (102) puede verificar la autenticidad del cliente verificando la firma aplicada al mensaje y comparando el ID de la lista blanca del cliente con los ID de la lista blanca de las plataformas aprobadas (Pág. 6, Párr. 068).	Después del aprovisionamiento, el cliente (101) puede autenticarse en el servidor (102) desellando los secretos dentro del enclave seguro (304) y enviando su ID de lista blanca al servidor (102), por ejemplo, en un mensaje firmado. El servidor (102) puede verificar la autenticidad del cliente verificando la firma aplicada al mensaje y comparando el ID de la lista blanca del cliente con los ID de la lista blanca de las plataformas aprobadas (Pág. 9, Párr. 098).

De acuerdo con la tabla anterior, las características esenciales del sistema de la reivindicación 11 habían sido divulgadas previamente en los documentos D1 y D2, por lo tanto, la materia reivindicada no es nueva.

Asimismo, el documento D1 divulga las características de las reivindicaciones dependientes así:

- Reivindicación 12: La capacidad de una parte remota para verificar que las medidas del enclave y los ajustes de la plataforma estén configurados como se espera se conoce como atestación. SGX utiliza dos credenciales relacionadas para la certificación: informes y cotizaciones. Se usa un informe para verificar la exactitud de los enclaves en la plataforma local, y se puede usar una cotización para reflejar la plataforma y el estado del enclave a entidades fuera de la plataforma (Pág. 3, Párr. 039). Las instrucciones CPM también pueden hacer que el nodo (101) selle el ID de la lista blanca en el enclave de memoria (304) (Pág. 8, Párr. 085). Las instrucciones CPM también pueden hacer que el nodo (101) selle el ID de la lista blanca en el enclave de memoria (304), por ejemplo, cifrando el ID de la lista blanca con la clave del enclave de la memoria del enclave (304) (Pág. 8, Párr. 085).
- Reivindicación 13: A este respecto, el CPM (306) puede hacer que el nodo (101) envíe un reporte de enclave a un módulo de cotización como el módulo de cotización (307) (Pág. 5, Párr. 058). El nodo (101) y el nodo (102), respectivamente, incluyen plataformas de dispositivos (301), (308). Sin limitación, las plataformas de dispositivos (301), (308) pueden correlacionarse con uno o más tipos de dispositivos, como servidores, clientes, nodos de computación móvil, teléfonos inteligentes, tabletas, computadoras portátiles, netbooks y similares (Pág. 4, Párr. 043). El nodo (101) también puede incluir el módulo de cotización (307), que puede incluir instrucciones legibles por computadora que cuando se ejecutan (por ejemplo, por el procesador (302)) pueden hacer que el nodo (101) realice operaciones de verificación de informes de enclave y operaciones de generación de cotizaciones de enclave consistentes (Pág. 4, Párr. 052).

Oficio N° 9787 de 24 de junio de 2021

Ref. Expediente N° NC2019/0007656

- Reivindicación 14: A este respecto, el CPM (306) puede hacer que el nodo (101) envíe un reporte de enclave a un módulo de cotización como el módulo de cotización (307) (Pág. 5, Párr. 058). El nodo (102) puede verificar la autenticidad del cliente verificando la firma aplicada al mensaje y comparando el ID de la lista blanca del cliente con los ID de la lista blanca de las plataformas aprobadas. Debido a que el nodo (101) puede revelar los secretos dentro del enclave de memoria (304), el texto sin formato de dichos secretos puede protegerse de malware u otras entidades no autorizadas residentes en el cliente (101) (Pág. 6, Párr. 068).

Las reivindicaciones dependientes 12 a 14 tampoco cumplen con el requisito de novedad.

4.2 Nivel Inventivo (Art. 18 Decisión 486)

La reivindicación 15 consiste en: “El sistema de acuerdo con la reivindicación 11, en donde las instrucciones provocan además al menos:” (Radicado N° NC2019/0007656 del 16 de julio de 2019).

Tabla 4. Comparación de las características técnicas esenciales, con las del estado de la técnica:

Características esenciales	D1	D3
El sistema de acuerdo con la reivindicación 11, en donde las instrucciones provocan además al menos: (...)	El ejemplo 18 incluye un aparato que comprende: al menos una memoria; al menos un procesador, acoplado a la memoria, para realizar operaciones que comprenden (...) (Pág. 13, Párr. 150).	Una técnica para permitir una aplicación segura y la integridad de los datos dentro de un sistema informático. En una realización, se establecen uno o más enclaves seguros en los que se pueden almacenar y ejecutar una aplicación y datos (Pág. 1, Resumen).
Completar parcialmente una operación de procesamiento seguro en el enclave de origen.	La primera parte incluye un entorno de ejecución confiable (110) con capacidades de certificación como, sin limitación, un Intel® Secure Enclave (en ocasiones denominado Intel® Software Guard Extensions (Intel® SGX)), Intel® Management Engine (Intel® ME), y similares (Pág. 2, Párr. 019).	El bit de enclave se compara con el bit de modo de enclave. Los bits adicionales proporcionarían una funcionalidad de identificación de espacio enclave. A un enclave en particular se le asignaría una identificación. La identificación se compararía con la identificación del enclave en ejecución como parte de la verificación de la dirección (Pág. 3, Párr. 053).
En donde los datos de enclave incluyen datos de estado del enclave de origen suficientes para permitir que otra instanciación de enclave continúe la operación de procesamiento seguro completada parcialmente.	No se menciona	Si el evento fue una interrupción, el enclave entra en estado interrumpido. Si el evento fue una excepción, el enclave entra en el estado de excepciones. Estos dos estados se distinguen para garantizar la entrega de una excepción de enclave al enclave y también para evitar la entrega de una excepción espuria atacando el código de la aplicación (Pág. 33, Párr. 392).

El documento D1 se considera el estado de la técnica más cercano a la invención definida en la reivindicación 15 porque divulga un método ejecutado por al menos un procesador que comprende inicializar el primer y segundo enclaves seguros, cada uno de los cuales comprende un entorno de ejecución de software confiable que evita que el

Oficio N° 9787 de 24 de junio de 2021

Ref. Expediente N° NC2019/0007656

software que se ejecuta fuera del primer y segundo enclaves seguros tenga acceso a software y datos dentro del primer y segundo enclaves seguros (Pág. 1, Resumen).

La diferencia entre la invención definida en la reivindicación 15 y el sistema divulgado de D1 consiste en que los datos de enclave incluyen datos de estado del enclave de origen suficientes para permitir que otra instanciación de enclave continúe la operación de procesamiento seguro completada parcialmente.

El efecto que se logra al incluir que los datos de enclave incluyen datos de estado del enclave de origen suficientes para permitir que otra instanciación de enclave continúe la operación de procesamiento seguro completada parcialmente es permitir que un enclave se reinicie a un estado previo, que se interrumpa una operación de enclave seguro y continúe posteriormente en otro enclave.

Por lo tanto, el problema técnico objetivo que pretende resolver esta invención se puede formular así: ¿Cómo modificar el sistema conocido en D1 con el fin de permitir que un enclave se reinicie a un estado previo, que se interrumpa una operación de enclave seguro y continúe posteriormente en otro enclave?

Sin embargo, el incluir que los datos de enclave incluyen datos de estado del enclave de origen suficientes para permitir que otra instanciación de enclave continúe la operación de procesamiento seguro completada parcialmente para permitir que un enclave se reinicie a un estado previo, que se interrumpa una operación de enclave seguro y continúe posteriormente en otro enclave, ya está divulgado en el documento D3 que se refiere a que si el evento fue una interrupción, el enclave entra en estado interrumpido. Si el evento fue una excepción, el enclave entra en el estado de excepciones. Estos dos estados se distinguen para garantizar la entrega de una excepción de enclave al enclave y también para evitar la entrega de una excepción espuria atacando el código de la aplicación (Pág. 33, Párr. 392).

En consecuencia, la persona normalmente versada en la materia estaría motivada a incluir que los datos de enclave incluyen datos de estado del enclave de origen suficientes para permitir que otra instanciación de enclave continúe la operación de procesamiento seguro completada del documento D3 en el sistema de D1, para así llegar al objeto de la reivindicación 15. Por lo cual se considera obvia.

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	US 2015/347768	1 a 14	Novedad
		15	Nivel Inventivo
D2	US 2015/304736	1, 6 y 11	Novedad
D3	US 2013/198853	15	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 requerimiento, o si a pesar de la respuesta subsistieran los impedimentos para la concesión, se denegará la patente.



Oficio N° 9787 de 24 de junio de 2021

Ref. Expediente N° NC2019/0007656

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° 9787 de 24 de junio de 2021

Ref. Expediente N° NC2019/0007656

INFORME DE BÚSQUEDA
EXAMEN DE PATENTABILIDAD

Solicitud No.		Examen de patentabilidad							
NC2019/0007656		1°	X	2°		3°		Revoca	
Solicitud Internacional No.		Fecha solicitud internacional: (DD/MM/AÑO)							
PCT/US2017/067455		20 de diciembre de 2017							
Fecha de determinación estado de la técnica (DD/MM/AÑO)				Prioridad			Presentación		
24/01/2017				X					
Solicitante									
LLC MICROSOFT TECHNOLOGY LICENSING									
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 15
Palabras clave utilizadas	Enclave, list, seal, authenticat*, status, state
Clasificaciones utilizadas para la búsqueda	CIP: G06F 21/60, 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	16139041	30/09/2016	-	-	A
WO	US 2015/347768	03/12/2015	1 a 14	(Pág. 3, Párr. 039) (Pág. 4, Párr. 043) (Pág. 4, Párr. 052) (Pág. 5, Párr. 058) (Pág. 6, Párr. 068) (Pág. 7, Párr. 083) (Pág. 8, Párr. 085) (Pág. 10, Párr. 113) (Pág. 10, Párr. 114) (Pág. 11, Párr. 119)	X
			15	(Pág. 2, Párr. 019)	Y
			US 8176283	08/05/2012	-
USPTO	US 2016/335453	17/11/2016	-	-	A
	US 9584517	28/02/2017	-	-	T
	US 2017/288875	05/10/2017	-	-	T
	US 2018/096137	05/04/2018	-	-	T
	US 2015/033012	29/01/2015	-	-	A
	US 8438631	07/05/2013	-	-	A
	US 2013/312117	21/11/2013	-	-	A
	US 2017/185752	29/06/2017	-	-	T
	US 2008/077994	27/03/2008	-	-	A
	US 2017/185766	29/06/2017	-	-	T
	US 2016/149912	26/05/2016	-	-	A
	US 2015/200949	16/07/2015	-	-	A
US 2010/154032	17/06/2010	-	-	A	

Oficio N° 9787 de 24 de junio de 2021

Ref. Expediente N° NC2019/0007656

Patbase	US 2015/304736	22/10/2015	1, 6 y 11	(Pág. 8, Párr. 089) (Pág. 9, Párr. 096) (Pág. 9, Párr. 098) (Pág. 11, Párr. 113) (Pág. 10, Párr. 115)	X
	US 2013/198853	01/08/2013	15	(Pág. 3, Párr. 053) (Pág. 33, Párr. 392)	Y
(1) Cita completa literatura no patente (LNP)					
Apellido, A. A. (Fecha). Título del artículo. <i>Nombre de la revista</i> . 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. “E” Solicitud de patente o patente anterior pero publicada en la fecha de presentación internacional o en fecha posterior. “L” Documento citado para llamar la atención sobre por ejemplo, dudas acerca de una reivindicación de prioridad o para determinar la fecha de publicación de otra cita, siempre van acompañados de una explicación, por la cual se citan. “O” Documento del tipo actas de conferencia, este tipo de documentos siempre estará acompañado por otra letra que indique la pertinencia del documento, por ejemplo, O,X, O,Y o bien O,A. “P” Documento publicado antes de la fecha de presentación internacional pero con posterioridad a la fecha de prioridad reivindicada. “T” Documento publicado en fecha posterior a la de presentación o la de prioridad de la solicitud internacional y no entra en conflicto con dicha solicitud, pero puede ser útil para la mejor comprensión del principio o teoría en que se basa la invención, o para demostrar que el razonamiento o los hechos en los que se basa dicha invención son incorrectos. “X” Documento particularmente relevante; la invención reivindicada no puede considerarse nueva o que implique una actividad inventiva por referencia al documento aisladamente considerado. “Y” Documento particularmente relevante; la invención reivindicada no puede considerarse que implique una actividad inventiva cuando el documento se asocia a otro u otros documentos de la misma naturaleza, cuya combinación resulta evidente para un experto en la materia.					
Fecha del reporte de búsqueda: 03/05/2021					
Examinador: FERNANDO NICOLÁS VARGAS PLAZAS					