

REPÚBLICA DE COLOMBIA
SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO

Oficio N° 11103 de 14 de julio de 2021

Ref. Expediente N° NC2019/0009852

Señor(a)
LLC MICROSOFT TECHNOLOGY LICENSING

TÍTULO DE LA SOLICITUD: ***“OFUSCACIÓN DEL CONTENIDO DE USUARIO EN ARCHIVOS DE DATOS ESTRUCTURADOS DE USUARIO”***

NÚMERO DE SOLICITUD INTERNACIONAL: PCT/US2018/022767.

FECHA DE PRESENTACIÓN INTERNACIONAL: 16 de marzo de 2018.

PRIORIDAD(ES): US, 15/467,029, 23 de marzo de 2017.

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° NC2019/0009852 del 11 de septiembre de 2019.

El problema planteado en esta solicitud consiste en la necesidad de identificar contenido confidencial dentro de documentos para servicios de protección contra pérdida de datos.

Para resolver este problema técnico, la solicitud en estudio proporciona sistemas y métodos para estructuras de ofuscación de datos para aplicaciones de usuario. Un método ejemplar incluye proporcionar contenido de usuario a un servicio de clasificación configurado para procesar el contenido de usuario para clasificar porciones del contenido de usuario como que incluyen contenido confidencial, y recibir del servicio de clasificación indicaciones del contenido de usuario que incluye contenido confidencial. El método incluye presentar indicaciones gráficas en una interfaz de usuario a la aplicación de usuario que anotan el contenido de usuario como que incluye contenido confidencial, y presentar opciones de ofuscación en la interfaz de usuario para ocultar el contenido confidencial dentro de al menos una porción seleccionada entre el contenido de usuario. En respuesta a una selección de usuario de al menos una de las opciones de ofuscación, el método incluye reemplazar el contenido de usuario asociado con contenido ofuscado que mantiene un esquema de datos del contenido de usuario asociado (Resumen).

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



Oficio N° 11103 de 14 de julio de 2021

Ref. Expediente N° NC2019/0009852

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° NC2019/0009852 el 11 de septiembre de 2019, tituló la invención como: “OFUSCACIÓN DEL CONTENIDO DE USUARIO EN ARCHIVOS DE DATOS ESTRUCTURADOS DE USUARIO”. 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 ESTRUCTURA DE OFUSCACIÓN DEL CONTENIDO DE USUARIO EN ARCHIVOS DE DATOS ESTRUCTURADOS DE USUARIO”.

3. Determinación del Estado de la Técnica

La fecha para determinar el estado de la técnica es el 23 de marzo de 2017 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	US20090132419	“Obfuscating sensitive data while preserving data usability”	21 de mayo de 2009

El documento D1¹ divulga un método y sistema para ofuscar datos confidenciales mientras se preserva la usabilidad de los datos. Se identifican los archivos de datos dentro del alcance de una aplicación. Los archivos de datos incluidos en el alcance incluyen datos confidenciales que deben enmascarse para preservar su confidencialidad. Se recopilan las definiciones de datos. Se identifican los campos de datos sensibles primarios. Los nombres de datos para los campos de datos sensibles primarios están normalizados. Los campos de datos sensibles primarios se clasifican según la sensibilidad. Los métodos de enmascaramiento apropiados se seleccionan de un conjunto predefinido que se aplicará a cada elemento de datos en función de las reglas ejercidas sobre los datos. Los datos que se enmascaran se perfilan para detectar datos no válidos. Se desarrolla software de enmascaramiento y se aplican consideraciones de entrada. Se ejecuta el método de enmascaramiento seleccionado y se realiza la validación operativa y funcional (Resumen).

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

4.1. Novedad (Art 16 Decisión 486)

La reivindicación 1 consiste en: “Un método para proporcionar una estructura de ofuscación de datos (...)” (Radicado N° NC2019/0009852 del 11 de septiembre de 2019).

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

Características esenciales	D1
Un método para proporcionar una estructura de ofuscación de datos para una aplicación de usuario, el método que comprende.	Un método y sistema de ofuscación de datos sensibles y más particularmente a una técnica para enmascarar datos sensibles para asegurar la confidencialidad del usuario final y / o la seguridad de la red mientras se preserva la usabilidad de los datos en las aplicaciones de software (Pág. 1, Párr. 0001).
Proporcionar contenido de usuario a un servicio de	Un producto de programa informático y un proceso para soportar la infraestructura informática que proporciona al menos un servicio

¹<https://patentimages.storage.googleapis.com/27/46/41/3b2a7629e4d0da/US20090132419A1.pdf>

Oficio N° 11103 de 14 de julio de 2021

Ref. Expediente N° NC2019/0009852

clasificación configurado para procesar el contenido de usuario para clasificar porciones del contenido de usuario como que comprende contenido confidencial correspondiente a uno o más esquemas de datos predeterminados.	de soporte correspondiente al método resumido anteriormente (Pág. 1, Párr. 0008). La presente invención puede proporcionar un proceso de enmascaramiento de datos (también conocido como ofuscación de datos) consistente y repetible que permite a toda una empresa ejecutar la solución de enmascaramiento de datos en diferentes aplicaciones (Pág. 3, Párr. 0056, líneas 14 a 18). Clasificar la pluralidad de datos sensibles primarios elementos en una pluralidad de categorías de confidencialidad de datos (Pág. 2, Párr. 0018, líneas 1 a 2). Las clasificaciones del cuadro (500) están ordenadas por nivel de sensibilidad del elemento de datos, donde 1 identifica los elementos de datos que tienen los valores de datos más sensibles (es decir, el mayor riesgo de seguridad de los datos) y 4 identifica los elementos de datos que tienen los valores de datos menos sensibles (Pág. 5, Párr. 0095, líneas 4 a 8). Uno o más de los campos de datos confidenciales primarios incluyen valores de datos confidenciales, que se definen como valores de datos preenmascarados que tienen un riesgo de seguridad que excede un nivel de riesgo predeterminado (Pág. 4, Párr. 0075, líneas 8 a 11). Datos que se ingresan a la aplicación comercial y que deben enmascarse para preservar la confidencialidad de los datos (Pág. 3, Párr. 0058, líneas 4 a 6).															
Recibir del servicio de clasificación indicaciones de una o más porciones del contenido de usuario que contienen el contenido confidencial.	Un ejemplo del diagrama del alcance de la aplicación recibido en el paso (202) es el diagrama (300) de la figura 3. El diagrama (300) incluye la aplicación (302) en el centro de un universo que incluye una capa de actores (304) y una capa de datos de límites. (306). La capa (304) de actores incluye las personas y los procesos que proporcionan datos o reciben datos de la aplicación (302) (Pág. 4, Párr. 0065, líneas 1 a 6). Datos que se ingresan a la aplicación comercial y que deben enmascarse para preservar la confidencialidad de los datos (Pág. 3, Párr. 0058, líneas 4 a 6).															
Presentar indicaciones gráficas en una interfaz de usuario a la aplicación de usuario que anotan las una o más porciones del contenido de usuario como que incluyen contenido confidencial.	Los informes incluidos en la salida (115) pueden mostrarse en una pantalla de visualización (no se muestra) o pueden incluirse en una copia impresa del informe (Pág. 3, Párr. 0059, líneas 10 a 12). Los datos de origen (314) de la aplicación externa (310) se introducen en la aplicación (302) como lote o mediante una interfaz en tiempo real. Los datos de origen (314) son un candidato inicial para el enmascaramiento (Pág. 4, Párr. 0068). La figura 5 es una tabla de clasificaciones de sensibilidad de datos utilizadas en una etapa de clasificación del proceso de las figuras 2A-2B, de acuerdo con realizaciones de la presente invención (Pág. 2, Párr. 0045). <table><tr><th>CLASSIFICATION</th><th>DESCRIPTION</th><th>RISK CHARACTERISTICS</th></tr><tr><td>TYPE 1 PERSONALLY SENSITIVE</td><td>INFORMATION THAT CAN BE MISUSED TO HARM A PERSON IN A FINANCIAL, EMPLOYMENT OR SOCIAL WAY. (NAMES, SOCIAL SECURITY NUMBER, CREDIT CARD, ETC.)</td><td>HIGH: INFORMATION IS PUBLICLY AVAILABLE TO IDENTIFY AN INDIVIDUAL OR DIRECTLY MISUSE THE DATA ITSELF</td></tr><tr><td>TYPE 2 NETWORK SENSITIVE</td><td>INFORMATION THAT CAN BE MISUSED TO BREACH OR DISABLE CRITICAL NETWORK COMMUNICATION (CIRCUIT IDENTIFIERS, IP ADDRESSES, ETC.)</td><td>MEDIUM: INFORMATION IS NOT PUBLICLY AVAILABLE BUT MAY BE KNOWN TO EMPLOYEES AND CONTRACTORS AND CAN PLACE INFRASTRUCTURE AT RISK</td></tr><tr><td>TYPE 3 CORPORATE SENSITIVE</td><td>INFORMATION THAT CAN BE MISUSED TO COMPROMISE THE COMPETITIVE POSITION OF A COMPANY (OPERATIONAL METRICS, ETC.)</td><td>VARIES: INFERENCE RISK MUST BE ANALYZED ON A CASE-BY-CASE BASIS, DOCUMENTED, AND RAISED TO SECURITY STAKEHOLDER</td></tr><tr><td>TYPE 4 MISCELLANEOUS</td><td>FURTHER QUALIFIES A TYPE 1, 2 OR 3 ELEMENT THAT HAS NO INDEPENDENT VALUE</td><td>VARIES, BUT USUALLY SENSITIVE WHEN PAIRED WITH OTHER DATA</td></tr></table> Datos que se ingresan a la aplicación comercial y que deben enmascarse para preservar la confidencialidad de los datos (Pág. 3, Párr. 0058, líneas 4 a 6).	CLASSIFICATION	DESCRIPTION	RISK CHARACTERISTICS	TYPE 1 PERSONALLY SENSITIVE	INFORMATION THAT CAN BE MISUSED TO HARM A PERSON IN A FINANCIAL, EMPLOYMENT OR SOCIAL WAY. (NAMES, SOCIAL SECURITY NUMBER, CREDIT CARD, ETC.)	HIGH: INFORMATION IS PUBLICLY AVAILABLE TO IDENTIFY AN INDIVIDUAL OR DIRECTLY MISUSE THE DATA ITSELF	TYPE 2 NETWORK SENSITIVE	INFORMATION THAT CAN BE MISUSED TO BREACH OR DISABLE CRITICAL NETWORK COMMUNICATION (CIRCUIT IDENTIFIERS, IP ADDRESSES, ETC.)	MEDIUM: INFORMATION IS NOT PUBLICLY AVAILABLE BUT MAY BE KNOWN TO EMPLOYEES AND CONTRACTORS AND CAN PLACE INFRASTRUCTURE AT RISK	TYPE 3 CORPORATE SENSITIVE	INFORMATION THAT CAN BE MISUSED TO COMPROMISE THE COMPETITIVE POSITION OF A COMPANY (OPERATIONAL METRICS, ETC.)	VARIES: INFERENCE RISK MUST BE ANALYZED ON A CASE-BY-CASE BASIS, DOCUMENTED, AND RAISED TO SECURITY STAKEHOLDER	TYPE 4 MISCELLANEOUS	FURTHER QUALIFIES A TYPE 1, 2 OR 3 ELEMENT THAT HAS NO INDEPENDENT VALUE	VARIES, BUT USUALLY SENSITIVE WHEN PAIRED WITH OTHER DATA
CLASSIFICATION	DESCRIPTION	RISK CHARACTERISTICS														
TYPE 1 PERSONALLY SENSITIVE	INFORMATION THAT CAN BE MISUSED TO HARM A PERSON IN A FINANCIAL, EMPLOYMENT OR SOCIAL WAY. (NAMES, SOCIAL SECURITY NUMBER, CREDIT CARD, ETC.)	HIGH: INFORMATION IS PUBLICLY AVAILABLE TO IDENTIFY AN INDIVIDUAL OR DIRECTLY MISUSE THE DATA ITSELF														
TYPE 2 NETWORK SENSITIVE	INFORMATION THAT CAN BE MISUSED TO BREACH OR DISABLE CRITICAL NETWORK COMMUNICATION (CIRCUIT IDENTIFIERS, IP ADDRESSES, ETC.)	MEDIUM: INFORMATION IS NOT PUBLICLY AVAILABLE BUT MAY BE KNOWN TO EMPLOYEES AND CONTRACTORS AND CAN PLACE INFRASTRUCTURE AT RISK														
TYPE 3 CORPORATE SENSITIVE	INFORMATION THAT CAN BE MISUSED TO COMPROMISE THE COMPETITIVE POSITION OF A COMPANY (OPERATIONAL METRICS, ETC.)	VARIES: INFERENCE RISK MUST BE ANALYZED ON A CASE-BY-CASE BASIS, DOCUMENTED, AND RAISED TO SECURITY STAKEHOLDER														
TYPE 4 MISCELLANEOUS	FURTHER QUALIFIES A TYPE 1, 2 OR 3 ELEMENT THAT HAS NO INDEPENDENT VALUE	VARIES, BUT USUALLY SENSITIVE WHEN PAIRED WITH OTHER DATA														

Oficio N° 11103 de 14 de julio de 2021

Ref. Expediente N° NC2019/0009852

	La herramienta de software que gestiona la matriz de análisis de datos (106) recibe indicaciones de los campos de datos que se identifican como campos de datos sensibles primarios en el paso (206) (Pág. 4, Párr. 0075, líneas 11 a 14).
Presentar opciones de ofuscación en la interfaz de usuario para ocultar el contenido confidencial dentro de al menos una porción seleccionada entre las una o más porciones del contenido de usuario; y.	Además, uno o más actores (es decir, individuos y / o aplicaciones de interfaz) que pueden operar en los datos entregados por la aplicación comercial pueden funcionar correctamente (Pág. 3, Párr. 0053, líneas 11 a14). Seleccionar un método de enmascaramiento de un conjunto de métodos de enmascaramiento predefinidos basados en una o más reglas ejercidas en un elemento de datos sensibles primarios de la pluralidad de elementos de datos sensibles primarios, donde el elemento de datos sensibles primarios incluye uno o más valores de datos sensibles de la pluralidad de valores de datos sensibles (Pág. 1, Párr. 0006). Datos que se ingresan a la aplicación comercial y que deben enmascarse para preservar la confidencialidad de los datos (Pág. 3, Párr. 0058, líneas 4 a 6).
En respuesta a una selección de usuario de al menos una de las opciones de ofuscación, reemplazar el contenido de usuario asociado con contenido ofuscado que mantiene un esquema de datos del contenido de usuario asociado.	Ejecutando el método de enmascaramiento seleccionado para reemplazar los datos sensibles con datos ficticios para fines de almacenamiento o presentación (Pág. 3, Párr. 0056, líneas 6 a 9). Una regla (también conocida como regla de reemplazo universal) que requiere que cada instancia del valor pre-enmascarado debe ser reemplazada universalmente con un valor post-enmascarado correspondiente significa que todas y cada una de las ocurrencias de un valor pre-enmascarado deben ser reemplazadas consistentemente con un valor de post-enmascarado. Por ejemplo, una regla de reemplazo universal puede requerir que todas y cada una de las ocurrencias de "SMITH se reemplacen consistentemente con MILLER (Pág. 6, párr. 0117).

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.

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

- Reivindicación 2: Volviendo al paso (212) de la figura 2, la idoneidad del método de enmascaramiento seleccionado se basa en las reglas comerciales y/o las reglas de TI identificadas como aplicadas al elemento de datos que se analiza. Por ejemplo, un primer método de enmascaramiento en el conjunto predefinido de métodos de enmascaramiento asegura la unicidad, un segundo método de enmascaramiento asegura una distribución equitativa de datos, un tercer método de enmascaramiento refuerza la integridad referencial, etc. (Pág. 6, Párr. 0101). Si no se ejerce ninguna regla comercial o de TI sobre un elemento de datos que se analiza, el método de enmascaramiento predeterminado mostrado en la tabla (700) de la figura 7 se selecciona para el elemento de datos en el paso (212) (Pág. 6, Párr. 0109). La selección de un método de enmascaramiento predeterminado se anula si una regla comercial o de TI se aplica a un elemento de datos, como los requisitos de integridad referencial o un requisito de conjuntos de valores válidos. En tales casos, el método de enmascaramiento predeterminado se cambia a otro método de enmascaramiento incluido en el conjunto de métodos de enmascaramiento predefinidos y puede requerir una técnica de enmascaramiento más inteligente (por ejemplo, una tabla de búsqueda) (Pág. 6, Párr. 0110). Datos que se ingresan a la aplicación comercial y que deben enmascarse para preservar la confidencialidad de los datos (Pág. 3, Párr. 0058, líneas 4 a 6).

Oficio N° 11103 de 14 de julio de 2021

Ref. Expediente N° NC2019/0009852

- Reivindicación 3: Una vez que todos los trabajos de enmascaramiento de datos se desarrollan y prueban para realizar la ofuscación de datos en todos los archivos dentro del alcance de la aplicación, los trabajos de enmascaramiento de datos se coreografían en una secuencia de trabajo para ejecutarse de manera automatizada que considera cualquier dependencia entre los trabajos de enmascaramiento de datos. La secuencia de trabajo se ejecuta en el paso (224) para acceder a la ubicación de los datos desenmascarados en pre-ofuscación en los archivos de datos de alcance (102) (ver figura1), ejecutar las transformaciones de datos (es decir, métodos de enmascaramiento) para ofuscar los datos y colocar los enmascarados datos en una ubicación específica en post-ofuscación en archivos de datos de alcance (120) (ver Figura 1) (Pág. 8, Párr. 0161, líneas 3 a 13).
- Reivindicación 4: Una pluralidad de indicadores de dichos nombres de elementos de datos normalizados incluidos en dicha pluralidad de nombres de elementos de datos normalizados, en el que dicho almacenamiento incluye asociar, en una correspondencia de muchos a uno, dichos nombres de elementos de datos de dicha pluralidad de nombres de elementos de datos con dichos indicadores de dicha pluralidad de indicadores (Pág. 13, Reivindicación 3, líneas 11 a 16). Columna E: Nombre del elemento. El nombre del elemento de datos (por ejemplo, según lo especificado por un administrador de base de datos o programas que hacen referencia al elemento de datos) Columna F: ¿Contienen estos datos? Un indicador Sí si el elemento de datos contiene un elemento en la siguiente lista de elementos sensibles; de lo contrario se indica No (Pág. 11, Párr. 0217).
- Reivindicación 5: Los atributos de datos describen los datos. Por ejemplo, un atributo de datos puede describir la longitud de un elemento de datos, o si el elemento de datos es un carácter, numérico, decimal, con signo o formateado. Las siguientes consideraciones están relacionadas con los atributos de los datos (Pág. 5, Párr. 0081). Si el paso de consulta (812) determina que una regla requiere que el elemento de datos incluya solo datos numéricos, entonces el método de enmascaramiento aleatorio universal se selecciona en el paso (814) como el método de enmascaramiento que se aplicará al elemento de datos y al proceso de la figura 8 termina; de lo contrario, el paso (812) determina que el elemento de datos puede incluir datos no numéricos, el método de enmascaramiento autógeno de referencia cruzada se selecciona en el paso (816) y el proceso de la figura 8 finaliza (Pág. 7, Párr. 0118)
- Reivindicación 6: Una regla (también conocida como regla de reemplazo universal) que requiere que cada instancia del valor pre-enmascarado debe ser reemplazada universalmente con un valor post-enmascarado correspondiente significa que todas y cada una de las ocurrencias de un valor pre-enmascarado deben ser reemplazadas consistentemente con un post-enmascarado valor. Por ejemplo, una regla de reemplazo universal puede requerir que todas y cada una de las apariciones de "SMITH se reemplacen consistentemente con MILLER (Pág. 6, Párr. 0117). Por ejemplo, el operador de enmascaramiento de datos verifica la integridad del comportamiento operativo asegurándose de que (1) se ingresaron los archivos adecuados al proceso de enmascaramiento de datos, (2) los métodos de enmascaramiento se completaron con éxito para todos los archivos y (3) no se realizaron excepciones que no fueron fatales (Pág. 9, Párr. 0161). Datos que se ingresan a la aplicación comercial y que deben enmascarse para preservar la confidencialidad de los datos (Pág. 3, Párr. 0058, líneas 4 a 6). El resultado de la



Oficio N° 11103 de 14 de julio de 2021

Ref. Expediente N° NC2019/0009852

revisión realizada en el paso (214) es una dirección para continuar con el paso (216) (ver figura 2B) del proceso de enmascaramiento de datos, o requiere información adicional para incorporar en la matriz de análisis de datos (106) (ver figura 1) y en otra documentación del método de enmascaramiento almacenada por la herramienta de software que administra la matriz de análisis de datos. Como tal, el proceso del paso (214) puede ser iterativo (Pág. 7, Párr. 0128). En el paso (226), una prueba de regresión (124) (ver figura 1) de la aplicación con datos enmascarados en archivos de datos (120) post-ofuscación dentro del alcance (ver figura 1) valida el comportamiento funcional de la aplicación y valida la cobertura completa de la prueba. Los datos enmascarados de salida se devuelven al entorno de prueba del sistema y deben integrarse de nuevo en un ciclo de prueba completo, que se define por el alcance completo de la aplicación identificada en el paso (202) (véase la figura 2A). Esta necesidad de que los datos enmascarados se vuelvan a integrar en un ciclo de prueba completo se debe a que la validación simple y positiva de los datos enmascarados a los requisitos no implica que la aplicación pueda procesar esos datos con éxito. El comportamiento funcional de la aplicación debe ser el mismo cuando se procesa con datos ofuscados (Pág. 9, Párr. 0163).

- Reivindicación 7: El perfil de datos realizado por la herramienta analizadora de datos (104) (ver Figura 1) en el paso (216) incluye revisar y analizar minuciosamente los valores de datos reales para identificar patrones dentro de los datos que se analizan y permitir que las reglas de reemplazo caigan dentro de los patrones identificados. Además, la elaboración de perfiles realizada por la herramienta analizadora de datos (104) (véase la figura 1) incluye la detección de datos no válidos (es decir, datos que no siguen las reglas que deben seguir los datos de sustitución ofuscados). En respuesta a la detección de datos no válidos, los datos confusos corrigen las condiciones de error o la lógica de excepción omite dichos datos. Como ejemplo, el perfil en el paso (216) determina que los datos que se definen realmente no están presentes (Pág. 7, Párr. 0129, líneas 7 a 18). Uno o más de los campos de datos confidenciales primarios incluyen valores de datos confidenciales, que se definen como valores de datos preenmascarados que tienen un riesgo de seguridad que excede un nivel de riesgo predeterminado (Pág. 4, Párr. 0075, líneas 8 a 11).
- Reivindicación 8: La secuencia de trabajo se ejecuta en el paso (224) para acceder a la ubicación de los datos desenmascarados en la ofuscación previa en los archivos (102) de datos de alcance (ver figura 1), ejecutar las transformaciones de datos (es decir, métodos de enmascaramiento) para ofuscar los datos, y colocar los datos enmascarados en una ubicación específica en post-ofuscación en archivos de datos de alcance (120) (ver Figura 1). La ubicación de los datos enmascarados puede reemplazar los datos desenmascarados o los datos enmascarados pueden ser un conjunto de datos completamente nuevo que se puede introducir en un momento posterior. Una vez que se completa la ejecución de la secuencia de trabajo en el paso (224), la herramienta de enmascaramiento de datos (110) (ver figura 1) proporciona las herramientas (es decir, los informes almacenados en los repositorios (916), (918) y (920) de la figura 9) para permitir que uno o miembros del soporte de TI equipo (por ejemplo, un operador de enmascaramiento de datos) para verificar manualmente la integridad del comportamiento operativo de los trabajos de enmascaramiento de datos. Por ejemplo, el operador de enmascaramiento de datos verifica la integridad del comportamiento operativo asegurándose de que (1) se ingresaron los archivos adecuados en el proceso de enmascaramiento de datos, (2) los métodos de



Oficio N° 11103 de 14 de julio de 2021

Ref. Expediente N° NC2019/0009852

enmascaramiento se completaron con éxito para todos los archivos y (3) no se realizaron excepciones fatal (Pág. 8, Párr. 0160, líneas 8 a 15 y Pág. 9, Párr. 0160). Por ejemplo, cada elemento de datos de los elementos de datos sensibles primarios se clasifica en una de las cuatro clasificaciones predefinidas numeradas del 1 al 4 en la tabla (500) de la figura 5. Las clasificaciones del cuadro (500) están ordenadas por nivel de sensibilidad del elemento de datos, donde 1 identifica los elementos de datos que tienen los valores de datos más sensibles (es decir, el mayor riesgo de seguridad de los datos) y 4 identifica los elementos de datos que tienen los valores de datos menos sensibles. Los elementos de datos que tienen los valores de datos más sensibles son aquellos elementos de datos que son identificadores directos y pueden contener información disponible en el dominio público. Los elementos de datos que son identificadores directos pero que no son inteligentes (p. Ej., Identificadores de circuitos) son tan sensibles como otros identificadores directos, pero se clasifican en la tabla (500) con un nivel de sensibilidad de 2. Claves únicas y no inteligentes (p. Ej., Números de clientes) se clasifican en el nivel de sensibilidad más bajo (Pág. 5, Párr. 0095, líneas 1 a 11).

Las reivindicaciones dependientes 2 a 8 tampoco cumplen con el requisito de novedad.

La reivindicación 9 consiste en: “Una estructura de ofuscación de datos para una aplicación de (...)” (Radicado N° NC2019/0009852 del 11 de septiembre de 2019).

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

Características esenciales	D1
Una estructura de ofuscación de datos para una aplicación de usuario, que comprende.	Un método y sistema de ofuscación de datos sensibles y más particularmente a una técnica para enmascarar datos sensibles para asegurar la confidencialidad del usuario final y / o la seguridad de la red mientras se preserva la usabilidad de los datos en las aplicaciones de software (Pág. 1, Párr. 0001).
Uno o más medios de almacenamiento legibles por computadora.	La memoria (1504) puede comprender cualquier tipo conocido de almacenamiento de datos y/o medio de transmisión, incluido el almacenamiento masivo, medios magnéticos, medios ópticos, memoria de acceso aleatorio (RAM), memoria de solo lectura (ROM), una caché de datos, un objeto de datos, etc (Pág. 12, Párr. 0250, líneas 1 a 5).
Un sistema de procesamiento operativamente conectado a uno o más medios de almacenamiento legibles por computadora; e.	El sistema informático (1500) comprende generalmente una unidad central de procesamiento (CPU) (1502), una memoria (1504), una interfaz de entrada / salida (E / S) (1506) y un bus (1508). El sistema informático (1500) está acoplado a los dispositivos de E / S (1510), la unidad de almacenamiento (1512), el repositorio de captura de auditoría (116), el repositorio 118 de datos de control de validación y de informes y los archivos de datos posteriores a la ofuscación dentro del alcance (120). La CPU (1502) realiza funciones de cálculo y control del sistema informático (1500). La CPU (1502) puede comprender una única unidad de procesamiento o estar distribuida entre una o más unidades de procesamiento en una o más ubicaciones (por ejemplo, en un cliente y un servidor) (Pág. 12, Párr. 0249, líneas 4 a 14).
Instrucciones de programa almacenadas en uno o más medios de almacenamiento legibles por computadora que, con base al menos en ser leídas y ejecutadas por el sistema de procesamiento, dirigen el sistema de procesamiento al menos para.	Sistema de ejecución de instrucciones para proporcionar y facilitar las capacidades de la presente invención. Para los propósitos de esta descripción, un medio legible o utilizable por computadora puede ser cualquier aparato que pueda contener, almacenar, comunicar, propagar o transportar el programa para su uso por o en conexión con el sistema, aparato o dispositivo de ejecución de instrucciones (Pág. 12, Párr. 0255, líneas 5 a 11).

Proporcionar contenido de usuario a un servicio de clasificación configurado para procesar el contenido de usuario para clasificar porciones del contenido de usuario como que comprenden contenido confidencial correspondiente a uno o más esquemas de datos predeterminados	Un producto de programa informático y un proceso para soportar la infraestructura informática que proporciona al menos un servicio de soporte correspondiente al método resumido anteriormente (Pág. 1, Párr. 0008). La presente invención puede proporcionar un proceso de enmascaramiento de datos (también conocido como ofuscación de datos) consistente y repetible que permite a toda una empresa ejecutar la solución de enmascaramiento de datos en diferentes aplicaciones (Pág. 3, Párr. 0056, líneas 14 a 18). Clasificar la pluralidad de datos sensibles primarios elementos en una pluralidad de categorías de confidencialidad de datos (Pág. 2, Párr. 0018, líneas 1 a 2). Las clasificaciones del cuadro (500) están ordenadas por nivel de sensibilidad del elemento de datos, donde 1 identifica los elementos de datos que tienen los valores de datos más sensibles (es decir, el mayor riesgo de seguridad de los datos) y 4 identifica los elementos de datos que tienen los valores de datos menos sensibles (Pág. 5, Párr. 0095, líneas 4 a 8). Uno o más de los campos de datos confidenciales primarios incluyen valores de datos confidenciales, que se definen como valores de datos preenmascarados que tienen un riesgo de seguridad que excede un nivel de riesgo predeterminado (Pág. 4, Párr. 0075, líneas 8 a 11). Datos que se ingresan a la aplicación comercial y que deben enmascarse para preservar la confidencialidad de los datos (Pág. 3, Párr. 0058, líneas 4 a 6).															
Recibir del servicio de clasificación indicaciones de una o más porciones del contenido de usuario que incluyen contenido confidencial.	Un ejemplo del diagrama del alcance de la aplicación recibido en el paso (202) es el diagrama (300) de la figura 3. El diagrama (300) incluye la aplicación (302) en el centro de un universo que incluye una capa de actores (304) y una capa de datos de límites. (306). La capa (304) de actores incluye las personas y los procesos que proporcionan datos o reciben datos de la aplicación (302) (Pág. 4, Párr. 0065, líneas 1 a 6). Datos que se ingresan a la aplicación comercial y que deben enmascarse para preservar la confidencialidad de los datos (Pág. 3, Párr. 0058, líneas 4 a 6).															
Presentar indicaciones gráficas en una interfaz de usuario a la aplicación de usuario que anotan las una o más porciones del contenido de usuario como que incluyen contenido confidencial.	Los informes incluidos en la salida (115) pueden mostrarse en una pantalla de visualización (no se muestra) o pueden incluirse en una copia impresa del informe (Pág. 3, Párr. 0059, líneas 10 a 12). Los datos de origen (314) de la aplicación externa (310) se introducen en la aplicación (302) como lote o mediante una interfaz en tiempo real. Los datos de origen (314) son un candidato inicial para el enmascaramiento (Pág. 4, Párr. 0068). Datos que se ingresan a la aplicación comercial y que deben enmascarse para preservar la confidencialidad de los datos (Pág. 3, Párr. 0058, líneas 4 a 6). La figura 5 es una tabla de clasificaciones de sensibilidad de datos utilizadas en una etapa de clasificación del proceso de las figuras 2A-2B, de acuerdo con realizaciones de la presente invención (Pág. 2, Párr. 0045). <table><tr><th>CLASSIFICATION</th><th>DESCRIPTION</th><th>RISK CHARACTERISTICS</th></tr><tr><td>TYPE 1 PERSONALLY SENSITIVE</td><td>INFORMATION THAT CAN BE MISUSED TO HARM A PERSON IN A FINANCIAL, EMPLOYMENT OR SOCIAL WAY. (NAMES, SOCIAL SECURITY NUMBER, CREDIT CARD, ETC.)</td><td>HIGH: INFORMATION IS PUBLICLY AVAILABLE TO IDENTIFY AN INDIVIDUAL OR DIRECTLY MISUSE THE DATA ITSELF</td></tr><tr><td>TYPE 2 NETWORK SENSITIVE</td><td>INFORMATION THAT CAN BE MISUSED TO BREACH OR DISABLE CRITICAL NETWORK COMMUNICATION (CIRCUIT IDENTIFIERS, IP ADDRESSES, ETC.)</td><td>MEDIUM: INFORMATION IS NOT PUBLICLY AVAILABLE BUT MAY BE KNOWN TO EMPLOYEES AND CONTRACTORS AND CAN PLACE INFRASTRUCTURE AT RISK</td></tr><tr><td>TYPE 3 CORPORATE SENSITIVE</td><td>INFORMATION THAT CAN BE MISUSED TO COMPROMISE THE COMPETITIVE POSITION OF A COMPANY (OPERATIONAL METRICS, ETC.)</td><td>VARIES: INFERENCE RISK MUST BE ANALYZED ON A CASE-BY-CASE BASIS, DOCUMENTED, AND RAISED TO SECURITY STAKEHOLDER</td></tr><tr><td>TYPE 4 MISCELLANEOUS</td><td>FURTHER QUALIFIES A TYPE 1, 2 OR 3 ELEMENT THAT HAS NO INDEPENDENT VALUE</td><td>VARIES, BUT USUALLY SENSITIVE WHEN PAIRED WITH OTHER DATA</td></tr></table>	CLASSIFICATION	DESCRIPTION	RISK CHARACTERISTICS	TYPE 1 PERSONALLY SENSITIVE	INFORMATION THAT CAN BE MISUSED TO HARM A PERSON IN A FINANCIAL, EMPLOYMENT OR SOCIAL WAY. (NAMES, SOCIAL SECURITY NUMBER, CREDIT CARD, ETC.)	HIGH: INFORMATION IS PUBLICLY AVAILABLE TO IDENTIFY AN INDIVIDUAL OR DIRECTLY MISUSE THE DATA ITSELF	TYPE 2 NETWORK SENSITIVE	INFORMATION THAT CAN BE MISUSED TO BREACH OR DISABLE CRITICAL NETWORK COMMUNICATION (CIRCUIT IDENTIFIERS, IP ADDRESSES, ETC.)	MEDIUM: INFORMATION IS NOT PUBLICLY AVAILABLE BUT MAY BE KNOWN TO EMPLOYEES AND CONTRACTORS AND CAN PLACE INFRASTRUCTURE AT RISK	TYPE 3 CORPORATE SENSITIVE	INFORMATION THAT CAN BE MISUSED TO COMPROMISE THE COMPETITIVE POSITION OF A COMPANY (OPERATIONAL METRICS, ETC.)	VARIES: INFERENCE RISK MUST BE ANALYZED ON A CASE-BY-CASE BASIS, DOCUMENTED, AND RAISED TO SECURITY STAKEHOLDER	TYPE 4 MISCELLANEOUS	FURTHER QUALIFIES A TYPE 1, 2 OR 3 ELEMENT THAT HAS NO INDEPENDENT VALUE	VARIES, BUT USUALLY SENSITIVE WHEN PAIRED WITH OTHER DATA
CLASSIFICATION	DESCRIPTION	RISK CHARACTERISTICS														
TYPE 1 PERSONALLY SENSITIVE	INFORMATION THAT CAN BE MISUSED TO HARM A PERSON IN A FINANCIAL, EMPLOYMENT OR SOCIAL WAY. (NAMES, SOCIAL SECURITY NUMBER, CREDIT CARD, ETC.)	HIGH: INFORMATION IS PUBLICLY AVAILABLE TO IDENTIFY AN INDIVIDUAL OR DIRECTLY MISUSE THE DATA ITSELF														
TYPE 2 NETWORK SENSITIVE	INFORMATION THAT CAN BE MISUSED TO BREACH OR DISABLE CRITICAL NETWORK COMMUNICATION (CIRCUIT IDENTIFIERS, IP ADDRESSES, ETC.)	MEDIUM: INFORMATION IS NOT PUBLICLY AVAILABLE BUT MAY BE KNOWN TO EMPLOYEES AND CONTRACTORS AND CAN PLACE INFRASTRUCTURE AT RISK														
TYPE 3 CORPORATE SENSITIVE	INFORMATION THAT CAN BE MISUSED TO COMPROMISE THE COMPETITIVE POSITION OF A COMPANY (OPERATIONAL METRICS, ETC.)	VARIES: INFERENCE RISK MUST BE ANALYZED ON A CASE-BY-CASE BASIS, DOCUMENTED, AND RAISED TO SECURITY STAKEHOLDER														
TYPE 4 MISCELLANEOUS	FURTHER QUALIFIES A TYPE 1, 2 OR 3 ELEMENT THAT HAS NO INDEPENDENT VALUE	VARIES, BUT USUALLY SENSITIVE WHEN PAIRED WITH OTHER DATA														

Oficio N° 11103 de 14 de julio de 2021

Ref. Expediente N° NC2019/0009852

	Datos que se ingresan a la aplicación comercial y que deben enmascarse para preservar la confidencialidad de los datos (Pág. 3, Párr. 0058, líneas 4 a 6). La herramienta de software que gestiona la matriz de análisis de datos (106) recibe indicaciones de los campos de datos que se identifican como campos de datos sensibles primarios en el paso (206) (Pág. 4, Párr. 0075, líneas 11 a 14).
Presentar opciones de ofuscación en la interfaz de usuario para ocultar el contenido confidencial dentro de al menos una porción seleccionada entre las una o más porciones del contenido de usuario; y.	Además, uno o más actores (es decir, individuos y / o aplicaciones de interfaz) que pueden operar en los datos entregados por la aplicación comercial pueden funcionar correctamente (Pág. 3, Párr. 0053, líneas 11 a14). Datos que se ingresan a la aplicación comercial y que deben enmascarse para preservar la confidencialidad de los datos (Pág. 3, Párr. 0058, líneas 4 a 6). Seleccionar un método de enmascaramiento de un conjunto de métodos de enmascaramiento predefinidos basados en una o más reglas ejercidas en un elemento de datos sensibles primarios de la pluralidad de elementos de datos sensibles primarios, donde el elemento de datos sensibles primarios incluye uno o más valores de datos sensibles de la pluralidad de valores de datos sensibles (Pág. 1, Párr. 0006).
En respuesta a una selección de usuario de al menos una de las opciones de ofuscación, reemplazar el contenido de usuario asociado con contenido ofuscado que mantiene un esquema de datos del contenido de usuario asociado.	Ejecutando el método de enmascaramiento seleccionado para reemplazar los datos sensibles con datos ficticios para fines de almacenamiento o presentación (Pág. 3, Párr. 0056, líneas 6 a 9). Una regla (también conocida como regla de reemplazo universal) que requiere que cada instancia del valor pre-enmascarado debe ser reemplazada universalmente con un valor post-enmascarado correspondiente significa que todas y cada una de las ocurrencias de un valor pre-enmascarado deben ser reemplazadas consistentemente con un valor de post-enmascarado. Por ejemplo, una regla de reemplazo universal puede requerir que todas y cada una de las ocurrencias de "SMITH se reemplacen consistentemente con MILLER (Pág. 6, párr. 0117).

De acuerdo con la tabla anterior, las características esenciales de la estructura de ofuscación de datos de la reivindicación 9 habían sido divulgadas previamente en el documento D1, por lo tanto, la materia reivindicada no es nueva.

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

- Reivindicación 10: Sistema de ejecución de instrucciones para proporcionar y facilitar las capacidades de la presente invención (Pág. 12, Párr. 0255, líneas 5 a 7). Volviendo al paso (212) de la figura 2, la idoneidad del método de enmascaramiento seleccionado se basa en las reglas comerciales y/o las reglas de TI identificadas como aplicadas al elemento de datos que se analiza. Por ejemplo, un primer método de enmascaramiento en el conjunto predefinido de métodos de enmascaramiento asegura la unicidad, un segundo método de enmascaramiento asegura una distribución equitativa de datos, un tercer método de enmascaramiento refuerza la integridad referencial, etc. (Pág. 6, Párr. 0101). Si no se ejerce ninguna regla comercial o de TI sobre un elemento de datos que se analiza, el método de enmascaramiento predeterminado mostrado en la tabla (700) de la figura 7 se selecciona para el elemento de datos en el paso (212) (Pág. 6, Párr. 0109). La selección de un método de enmascaramiento predeterminado se anula si una regla comercial o de TI se aplica a un elemento de datos, como los requisitos de integridad referencial o un requisito de conjuntos de valores válidos. En tales casos, el método de enmascaramiento predeterminado se cambia a otro método de enmascaramiento incluido en el conjunto de métodos de

Oficio N° 11103 de 14 de julio de 2021

Ref. Expediente N° NC2019/0009852

enmascaramiento predefinidos y puede requerir una técnica de enmascaramiento más inteligente (por ejemplo, una tabla de búsqueda) (Pág. 6, Párr. 0110). Una vez que todos los trabajos de enmascaramiento de datos se desarrollan y prueban para realizar la ofuscación de datos en todos los archivos dentro del alcance de la aplicación, los trabajos de enmascaramiento de datos se coreografían en una secuencia de trabajo para ejecutarse de manera automatizada que considera cualquier dependencia entre los trabajos de enmascaramiento de datos. La secuencia de trabajo se ejecuta en el paso (224) para acceder a la ubicación de los datos desenmascarados en pre-ofuscación en los archivos de datos de alcance (102) (ver figura1), ejecutar las transformaciones de datos (es decir, métodos de enmascaramiento) para ofuscar los datos y colocar los enmascarados datos en una ubicación específica en post-ofuscación en archivos de datos de alcance (120) (ver Figura 1) (Pág. 8, Párr. 0161, líneas 3 a 13). Datos que se ingresan a la aplicación comercial y que deben enmascarse para preservar la confidencialidad de los datos (Pág. 3, Párr. 0058, líneas 4 a 6).

- Reivindicación 11: Una pluralidad de indicadores de dichos nombres de elementos de datos normalizados incluidos en dicha pluralidad de nombres de elementos de datos normalizados, en el que dicho almacenamiento incluye asociar, en una correspondencia de muchos a uno, dichos nombres de elementos de datos de dicha pluralidad de nombres de elementos de datos con dichos indicadores de dicha pluralidad de indicadores (Pág. 13, Reivindicación 3, líneas 11 a 16). Columna E: Nombre del elemento. El nombre del elemento de datos (por ejemplo, según lo especificado por un administrador de base de datos o programas que hacen referencia al elemento de datos) Columna F: ¿Contienen estos datos? Un indicador Sí si el elemento de datos contiene un elemento en la siguiente lista de elementos sensibles; de lo contrario se indica No (Pág. 11, Párr. 0217).
- Reivindicación 12: Los atributos de datos describen los datos. Por ejemplo, un atributo de datos puede describir la longitud de un elemento de datos, o si el elemento de datos es un carácter, numérico, decimal, con signo o formateado. Las siguientes consideraciones están relacionadas con los atributos de los datos (Pág. 5, Párr. 0081). Si el paso de consulta (812) determina que una regla requiere que el elemento de datos incluya solo datos numéricos, entonces el método de enmascaramiento aleatorio universal se selecciona en el paso (814) como el método de enmascaramiento que se aplicará al elemento de datos y al proceso de la figura 8 termina; de lo contrario, el paso (812) determina que el elemento de datos puede incluir datos no numéricos, el método de enmascaramiento autógeno de referencia cruzada se selecciona en el paso (816) y el proceso de la figura 8 finaliza (Pág. 7, Párr. 0118)
- Reivindicación 13: Una regla (también conocida como regla de reemplazo universal) que requiere que cada instancia del valor pre-enmascarado debe ser reemplazada universalmente con un valor post-enmascarado correspondiente significa que todas y cada una de las ocurrencias de un valor pre-enmascarado deben ser reemplazadas consistentemente con un post-enmascarado valor. Por ejemplo, una regla de reemplazo universal puede requerir que todas y cada una de las apariciones de "SMITH se reemplacen consistentemente con MILLER (Pág. 6, Párr. 0117). Por ejemplo, el operador de enmascaramiento de datos Verifica la integridad del comportamiento operativo asegurándose de que (1) se ingresaron los archivos adecuados al proceso de enmascaramiento de datos, (2) los métodos de enmascaramiento se completaron con éxito para todos los archivos y (3) no se realizaron excepciones no fueron fatales (Pág. 9, Párr. 0161). Datos que se

Oficio N° 11103 de 14 de julio de 2021

Ref. Expediente N° NC2019/0009852

ingresan a la aplicación comercial y que deben enmascarse para preservar la confidencialidad de los datos (Pág. 3, Párr. 0058, líneas 4 a 6). El resultado de la revisión realizada en el paso (214) es una dirección para continuar con el paso (216) (ver figura 2B) del proceso de enmascaramiento de datos, o requiere información adicional para incorporar en la matriz de análisis de datos (106) (ver figura 1) y en otra documentación del método de enmascaramiento almacenada por la herramienta de software que administra la matriz de análisis de datos. Como tal, el proceso del paso (214) puede ser iterativo (Pág. 7, Párr. 0128). En el paso (226), una prueba de regresión (124) (ver figura 1) de la aplicación con datos enmascarados en archivos de datos (120) post-ofuscación dentro del alcance (ver figura 1) valida el comportamiento funcional de la aplicación y valida la cobertura completa de la prueba. Los datos enmascarados de salida se devuelven al entorno de prueba del sistema y deben integrarse de nuevo en un ciclo de prueba completo, que se define por el alcance completo de la aplicación identificada en el paso (202) (véase la figura 2A). Esta necesidad de que los datos enmascarados se vuelvan a integrar en un ciclo de prueba completo se debe a que la validación simple y positiva de los datos enmascarados a los requisitos no implica que la aplicación pueda procesar esos datos con éxito. El comportamiento funcional de la aplicación debe ser el mismo cuando se procesa con datos ofuscados (Pág. 9, Párr. 0163).

- Reivindicación 14: El perfil de datos realizado por la herramienta analizadora de datos (104) (ver Figura 1) en el paso (216) incluye revisar y analizar minuciosamente los valores de datos reales para identificar patrones dentro de los datos que se analizan y permitir que las reglas de reemplazo caigan dentro de los patrones identificados. Además, la elaboración de perfiles realizada por la herramienta analizadora de datos (104) (véase la figura 1) incluye la detección de datos no válidos (es decir, datos que no siguen las reglas que deben seguir los datos de sustitución ofuscados). En respuesta a la detección de datos no válidos, los datos confusos corrigen las condiciones de error o la lógica de excepción omite dichos datos. Como ejemplo, el perfil en el paso (216) determina que los datos que se definen realmente no están presentes (Pág. 7, Párr. 0129, líneas 7 a 18). Uno o más de los campos de datos confidenciales primarios incluyen valores de datos confidenciales, que se definen como valores de datos preenmascarados que tienen un riesgo de seguridad que excede un nivel de riesgo predeterminado (Pág. 4, Párr. 0075, líneas 8 a 11).
- Reivindicación 15: La secuencia de trabajo se ejecuta en el paso (224) para acceder a la ubicación de los datos desenmascarados en la ofuscación previa en los archivos (102) de datos de alcance (ver figura 1), ejecutar las transformaciones de datos (es decir, métodos de enmascaramiento) para ofuscar los datos, y colocar los datos enmascarados en una ubicación específica en post-ofuscación en archivos de datos de alcance (120) (ver Figura 1). La ubicación de los datos enmascarados puede reemplazar los datos desenmascarados o los datos enmascarados pueden ser un conjunto de datos completamente nuevo que se puede introducir en un momento posterior. Una vez que se completa la ejecución de la secuencia de trabajo en el paso (224), la herramienta de enmascaramiento de datos (110) (ver figura 1) proporciona las herramientas (es decir, los informes almacenados en los repositorios (916), (918) y (920) de la figura 9) para permitir que uno o miembros del soporte de TI equipo (por ejemplo, un operador de enmascaramiento de datos) para verificar manualmente la integridad del comportamiento operativo de los trabajos de enmascaramiento de datos. Por ejemplo, el operador de enmascaramiento de datos verifica la integridad del



Oficio N° 11103 de 14 de julio de 2021

Ref. Expediente N° NC2019/0009852

comportamiento operativo asegurándose de que (1) se ingresaron los archivos adecuados en el proceso de enmascaramiento de datos, (2) los métodos de enmascaramiento se completaron con éxito para todos los archivos y (3) no se realizaron excepciones fatal (Pág. 8, Párr. 0160, líneas 8 a 15 y Pág. 9, Párr. 0160). Por ejemplo, cada elemento de datos de los elementos de datos sensibles primarios se clasifica en una de las cuatro clasificaciones predefinidas numeradas del 1 al 4 en la tabla (500) de la figura 5. Las clasificaciones del cuadro (500) están ordenadas por nivel de sensibilidad del elemento de datos, donde 1 identifica los elementos de datos que tienen los valores de datos más sensibles (es decir, el mayor riesgo de seguridad de los datos) y 4 identifica los elementos de datos que tienen los valores de datos menos sensibles. Los elementos de datos que tienen los valores de datos más sensibles son aquellos elementos de datos que son identificadores directos y pueden contener información disponible en el dominio público. Los elementos de datos que son identificadores directos pero que no son inteligentes (p. Ej., Identificadores de circuitos) son tan sensibles como otros identificadores directos, pero se clasifican en la tabla (500) con un nivel de sensibilidad de 2. Claves únicas y no inteligentes (p. Ej., Números de clientes) se clasifican en el nivel de sensibilidad más bajo (Pág. 5, Párr. 0095, líneas 1 a 11).

Las reivindicaciones dependientes 10 a 15 tampoco cumplen con el requisito de novedad.

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	US20090132419	1 a 15	Novedad

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

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

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



Edna Marcela Ramirez Orozco
DIRECTORA DE NUEVAS CREACIONES



Oficio N° 11103 de 14 de julio de 2021

Ref. Expediente N° NC2019/0009852

INFORME DE BÚSQUEDA
EXAMEN DE PATENTABILIDAD

Solicitud No.		Examen de patentabilidad							
NC2019/0009852		1°	X	2°		3°		Revoca	
Solicitud Internacional No.		Fecha solicitud internacional: (DD/MM/AÑO)							
PCT/US2018/022767		16 de marzo de 2018							
Fecha de determinación estado de la técnica (DD/MM/AÑO)				Prioridad		Presentación			
23/03/2017				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				Obfuscat*, user, content, structur, data, files, method, applications, classification, service, present*, graphical,					
Clasificaciones utilizadas para la búsqueda				CIP:	G06F 21/62, H04L 29/06, H04W 12/02, G06F 3/0484				
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	CO12027597	16/02/2012	-	-			A		
WIPO	US2012259877	11/10/2012	-	-			A		
	US2010042583	18/02/2010	-	-			A		
	US2012239540	20/09/2012	-	-			A		
	US2010205189	12/08/2010	-	-			A		
USPTO	US2009132419	21/05/2009	1 a 15	1 Pág. 1, Párr. 0001; Pág. 1, Pár. 0008; Pág. 3, Párr. 0056, líneas 14 a 18; Pág. 2, Párr. 0018, líneas 1 a 2; Pág. 5, Párr. 0095, líneas 4 a 8; Pág. 4, Párr. 0075, líneas 8 a 11; Pág. 3, Párr. 0058, líneas 4 a 6; Pág. 4, Párr. 0065, líneas 1 a 6; Pág. 3, Párr. 0058, líneas 4 a 6; Pág. 3, Párr. 0059, líneas 10 a 12; Pág. 4, Párr. 0068; Pág. 3, Párr. 0053, líneas 11 a 14; Pág. 3, Párr. 0058, líneas 4 a 6; Pág. 3, Párr. 0056, líneas 6 a 9; Pág. 6, párr. 0117; Pág. 2, Párr. 0045; Pág. 3, Párr. 0058, líneas 4 a 6; figura 5; Pág. 1, Párr. 0006. 2 Pág. 6, Párrs. 0101, 0109 y 0110; Pág. 3, Párr. 0058, líneas 4 a 6.			X		

Oficio N° 11103 de 14 de julio de 2021

Ref. Expediente N° NC2019/0009852

				3 Pág. 8, Párr. 0161, líneas 3 a 13. 4 Pág. 13, Reivindicación 3, líneas 11 a 16; Pág. 11, Párr. 0217. 5 Pág. 5, Párr. 0081; Pág. 7, Párr. 0118. 6 Pág. 6, Párr. 0117; Pág. 3, Párr. 0058, líneas 4 a 6; Pág. 7, Párr. 0128; Pág. 9, Párr. 0163. 7 Pág. 7, Párr. 0129, líneas 7 a 18; Pág. 4, Párr. 0075, líneas 8 a 11. 8 Pág. 8, Párr. 0160, líneas 8 a 15 y Pág. 9, Párr. 0160; Pág. 5, Párr. 0095, líneas 1 a 11. 9 Pág. 1, Párr. 0001; Pág. 12, Párr. 0250, líneas 1 a 5; Pág. 12, Párr. 0249, líneas 4 a 14; Pág. 12, Párr. 0255, líneas 5 a 11;Pág. 1, Párr. 0008; Pág. 3, Párr. 0056, líneas 14 a 18; Pág. 2, Párr. 0018, líneas 1 a 2; Pág. 5, Párr. 0095, líneas 4 a 8; Pág. 4, Párr. 0075, líneas 8 a 11; Pág. 3, Párr. 0058, líneas 4 a 6; Pág. 4, Párr. 0065, líneas 1 a 6; Pág. 3, Párr. 0058, líneas 4 a 6; Pág. 3, Párr. 0059, líneas 10 a 12; Pág. 4, Párr. 0068; Pág. 3, Párr. 0053, líneas 11 a 14; Pág. 3, Párr. 0058, líneas 4 a 6; Pág. 3, Párr. 0056, líneas 6 a 9; Pág. 6, párr. 0117; Pág. 2, Párr. 0045; Pág. 3, Párr. 0058, líneas 4 a 6; figura 5; Pág. 1, Párr. 0006. 10 Pág. 6, Párrs. 0101, 0109 y 0110; Pág. 8, Párr. 0161, líneas 3 a 13; Pág. 3, Párr. 0058, líneas 4 a 6. 11 Pág. 13, Reivindicación 3, líneas 11 a 16; Pág. 11, Párr. 0217. 12 Pág. 5, Párr. 0081; Pág. 7, Párr. 0118. 13	
--	--	--	--	---	--

Oficio N° 11103 de 14 de julio de 2021

Ref. Expediente N° NC2019/0009852

				Pág. 6, Párr. 0117; Pág. 3, Párr. 0058, líneas 4 a 6; Pág. 7, Párr. 0128; Pág. 9, Párr. 0163. 14 Pág. 7, Párr. 0129, líneas 7 a 18; Pág. 4, Párr. 0075, líneas 8 a 11. 15 Pág. 8, Párr. 0160, líneas 8 a 15 y Pág. 9, Párr. 0160; Pág. 5, Párr. 0095, líneas 1 a 11.	
	US8898796 B2	25/11/2014	-	-	A
	US9177174 B1	3/11/2015	-	-	A
	US9454675 B2	27/09/2016	-	-	A
	US2008181396	31/07/2008	-	-	A
	US2009100527	16/04/2009	-	-	A
	US2009132419	21/05/2009	-	-	A
	US2009132575 A1	21/05/2009	-	-	A
	US2009144829 A1	4/06/2009	-	-	A
	US2010063843 A1	11/03/2010	-	-	A
	US2011239113 A1	29/09/2011	-	-	A
	US2012030165 A1	2/02/2012	-	-	A
	US2012239540 A1	20/09/2012	-	-	A
	US2014075542 A1	13/03/2014	-	-	A
	US2014344569 A1	20/11/2014	-	-	A
	US2015040237 A1	5/02/2015	-	-	A
	US2016203331 A1	14/07/2016	-	-	A
	US2017132420 A1	11/05/2017	-	-	E
	US2017300635 A1	19/10/2017	-	-	E
	US2018004976A1	4/01/2018	-	-	E
Patbase	US2019007358	03/01/2019	-	-	E
Epoquenet	US2021105310	08/04/2021	-	-	E
Googlepatent	US9298878B2	29/03/2016	-	-	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. “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: 14/05/2021					
Examinador: Freddy Alexander Velandia Vivas					

Oficio N° **11103** de **14 de julio de 2021**

Ref. Expediente N° NC2019/0009852

