

REPÚBLICA DE COLOMBIA
SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO

Resolución N° 37956

Ref. Expediente N° NC2019/0009852

Por la cual se deniega una Patente de Invención

EL SUPERINTENDENTE DE INDUSTRIA Y COMERCIO

en ejercicio de sus facultades legales, en especial de las conferidas en el numeral 24 del artículo 3° del Decreto 4886 de 2011, y

CONSIDERANDO

Que mediante escrito radicado en esta Superintendencia el 11 de septiembre de 2019, con el N° NC2019/0009852, por LLC MICROSOFT TECHNOLOGY LICENSING, entró a fase nacional la solicitud de patente de invención titulada "OFUSCACIÓN DEL CONTENIDO DE USUARIO EN ARCHIVOS DE DATOS ESTRUCTURADOS DE USUARIO", que corresponde a la solicitud internacional PCT/US2018/022767 del 16 de marzo de 2018.

Que la solicitud fue publicada en la Gaceta de la Propiedad Industrial N° 873 el 30 de septiembre de 2019, sin que se hubieran presentado oposiciones por parte de terceros.

Que realizado el examen de fondo mediante Oficio N° 2, notificado el 4 de enero de 2022, se requirió al solicitante en los términos del artículo 45 de la Decisión 486 de la Comisión de la Comunidad Andina para que presentara respuesta a las observaciones de carácter técnico, relacionadas con la patentabilidad o cumplimiento de los requisitos establecidos por esta Decisión para la concesión de la patente.

Que el solicitante mediante escrito radicado bajo el N° NC2019/0009852 el 25 de marzo de 2022, respondió oportunamente el requerimiento formulado y presentó las reivindicaciones 1 a 20 que reemplazan las originalmente presentadas. Se acepta este último capítulo reivindicatorio presentado, comoquiera que se ajusta a las prescripciones contenidas en el artículo 34 de la Decisión 486.

Que en virtud de lo dispuesto en el artículo 14 de la Decisión 486 expedida por la Comisión de la Comunidad Andina *"Los países miembros otorgarán patentes para las invenciones, sean de producto o de procedimiento, en todos los campos de la tecnología, siempre que sean nuevas, tengan nivel inventivo y sean susceptibles de aplicación industrial"*.

Que en el presente caso las reivindicaciones 1 a 20 incluidas en el radicado bajo el N° NC2019/0009852 el 25 de marzo de 2022, no cumplen los requisitos indicados. Lo anterior, de acuerdo con las siguientes consideraciones:

Objeto de la invención

El problema técnico 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 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



Resolución N° 37956

Ref. Expediente N° NC2019/0009852

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.

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).

Novedad (Art 16 Decisión 486)

Según lo dispuesto en el artículo 16 de la Decisión 486: *“Una invención se considerará nueva cuando no está comprendida en el estado de la técnica.*

El estado de la técnica comprenderá todo lo que haya sido accesible al público por una descripción escrita u oral, utilización, comercialización o cualquier otro medio antes de la fecha de presentación de la solicitud de patente o, en su caso, de la prioridad reconocida”.

En el presente caso, el método reclamado en la solicitud no es nuevo, teniendo en cuenta que la reivindicación 1 está referida a: *“Un método (400) para proporcionar una estructura de ofuscación de datos para (...)”* (Radicado N° NC2019/0009852 del 25 de marzo de 2022).

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



Resolución N° 37956

Ref. Expediente N° NC2019/0009852

La siguiente tabla presenta la comparación entre las características técnicas esenciales de la solicitud estudiada, mencionadas en la reivindicación 1, y las reveladas en el documento D1 que representa el estado de la técnica:

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

Características esenciales	D1
Un método (400) para proporcionar una estructura de ofuscación de datos para una aplicación de usuario (111), 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 (410) contenido de usuario (115, 116, 117) que comprende un archivo de datos de usuario visible en la aplicación de usuario a.	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) (...). (Pág. 4, Párr. 0068).
Un servicio de clasificación (214) configurado para procesar el contenido de usuario para clasificar porciones (140) del contenido de usuario como que comprende contenido confidencial correspondiente a uno o más esquemas de datos predeterminados.	(...) un servicio de soporte (...). (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). 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).
Recibir (415) del servicio de clasificación indicaciones de ubicaciones dentro del archivo de datos de usuario 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). (...) para acceder a la ubicación de los datos desenmascarados en archivos de datos dentro del alcance previos a la ofuscación (102) (...) coloque los datos enmascarados en una ubicación específica en los archivos de datos dentro del alcance posteriores a la ofuscación (120) (...). (Pág. 8, Párr. 0161).
Antes de ocultar el contenido confidencial.	Los datos provisionales (318) son datos que pueden ser de entrada y salida (...). En un escenario en el que los datos provisionales (318) existían antes de que se enmascararan los datos de origen (314), dichos datos provisionales deben considerarse candidatos para el enmascaramiento. (Pág. 4, Párr. 0070).
Presentar (416) anotaciones gráficas visibles en una interfaz de usuario a la aplicación de usuario que anotan cada una de las una o más porciones del contenido de usuario en la interfaz 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).

Resolución N° 37956

Ref. Expediente N° NC2019/0009852

	<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> (Hoja 7, Fig. 5). 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).	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														
Presentar, en la interfaz de usuario (112), elementos de selección grafica que corresponden a las anotaciones gráficas e indican opciones de ofuscación para ocultar el contenido confidencial; 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 dentro de la interfaz de usuario de al menos una de las opciones de ofuscación en un elemento de selección gráfica para contenido de usuario asociado, reemplazar (418) al menos el contenido de usuario asociado con contenido ofuscado que mantiene un esquema de datos de al menos el 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).

Resolución N° 37956

Ref. Expediente N° NC2019/0009852

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).

- 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



Resolución N° 37956

Ref. Expediente N° NC2019/0009852

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 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.



Resolución N° 37956

Ref. Expediente N° NC2019/0009852

(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 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.

En el presente caso, la estructura reclamada en la solicitud no es nuevo, teniendo en cuenta que la reivindicación 9 está referida a: *“Una estructura de ofuscación de datos para una aplicación de usuario, que comprende (...)”* (Radicado N° NC2019/0009852 del 25 de marzo de 2022).



Resolución N° 37956

Ref. Expediente N° NC2019/0009852

La siguiente tabla presenta la comparación entre las características técnicas esenciales de la solicitud estudiada, mencionadas en la reivindicación 9, y las reveladas en el documento D1 que representa el 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 (410) contenido de usuario que comprende un archivo de datos de usuario visible en la aplicación de usuario a.	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) (...). (Pág. 4, Párr. 0068).
Un servicio de clasificación (124) configurado para procesar el contenido de usuario para clasificar porciones (140) del contenido de usuario como que comprenden contenido confidencial correspondiente a uno o más esquemas de datos predeterminados.	(...) un servicio de soporte (...). (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). 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).
Recibir (415) del servicio de clasificación (124) indicaciones de ubicaciones dentro del archivo de datos de usuario 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). (...) para acceder a la ubicación de los datos desenmascarados en archivos de datos dentro del alcance previos a la ofuscación (102) (...) coloque los

Resolución N° 37956

Ref. Expediente N° NC2019/0009852

	datos enmascarados en una ubicación específica en los archivos de datos dentro del alcance posteriores a la ofuscación (120) (...). (Pág. 8, Párr. 0161).															
Antes de ocultar el contenido confidencial.	Los datos provisionales (318) son datos que pueden ser de entrada y salida (...) En un escenario en el que los datos provisionales (318) existían antes de que se enmascararan los datos de origen (314), dichos datos provisionales deben considerarse candidatos para el enmascaramiento. (Pág. 4, Párr. 0070).															
Presentar (416) anotaciones gráficas visibles en una interfaz de usuario a la aplicación de usuario que anotan cada una de las una o más porciones del contenido de usuario en la interfaz 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 border="1"><thead><tr><th>CLASSIFICATION</th><th>DESCRIPTION</th><th>RISK CHARACTERISTICS</th></tr></thead><tbody><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></tbody></table> (Hoja 7, Fig. 5). 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).	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														
Presentar, en la interfaz de usuario, elementos de selección grafica que corresponden a las anotaciones gráficas e indican opciones de ofuscación para ocultar el contenido confidencial.	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 dentro de la interfaz de usuario de al menos una de las opciones de ofuscación en un elemento de selección gráfica para contenido de usuario asociado, reemplazar (418) al menos el contenido de usuario asociado con contenido ofuscado que mantiene un esquema de datos de al menos el 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).															

Resolución N° 37956

Ref. Expediente N° NC2019/0009852

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 enmascaramiento predefinidos y puede requerir una técnica de enmascaramiento más inteligente (por ejemplo, una tabla de búsqueda).
(Pág. 6, Párr. 0110).
- Reivindicación 11: 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 12: 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,

Resolución N° 37956

Ref. Expediente N° NC2019/0009852

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 13: 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 14: 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 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

Resolución N° 37956

Ref. Expediente N° NC2019/0009852

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 15: 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 16: 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 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



Resolución N° 37956

Ref. Expediente N° NC2019/0009852

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 16 tampoco cumplen con el requisito de novedad.

En el presente caso, el método reclamado en la solicitud no es nuevo, teniendo en cuenta que la reivindicación 17 está referida a: *Un método para operar una aplicación de usuario de ofuscación de datos, el método que comprende (...)*” (Radicado N° NC2019/0009852 del 25 de marzo de 2022).

La siguiente tabla presenta la comparación entre las características técnicas esenciales de la solicitud estudiada, mencionadas en la reivindicación 17, y las reveladas en el documento D1 que representa el estado de la técnica:

Tabla 3. Comparación de las características técnicas esenciales, con las del estado de la técnica	
Características esenciales	D1
Un método para operar una aplicación de usuario de ofuscación de datos, el método que comprende.	Un método (...) en las aplicaciones de software. (Pág. 1, Párr. 0001). (...) un primer usuario (308) y un proceso que proporciona datos a la aplicación (302) incluyen una primera aplicación externa (310). (Párr. 0065).
Proporcionar (410) contenido de usuario de un archivo de datos de usuario.	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) (...). (Pág. 4, Párr. 0068).
A un servicio de clasificación (124) configurado para procesar el contenido de usuario para clasificar una o más porciones del contenido de usuario como que comprende contenido confidencial correspondiente a uno o más esquemas de datos.	(...) un servicio de soporte (...). (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). 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).
Antes de ocultar el contenido confidencial.	Los datos provisionales (318) son datos que pueden ser de entrada y salida (...). En un escenario en el que los datos provisionales (318) existían antes de que se enmascararan los datos de origen (314), dichos datos provisionales deben considerarse candidatos para el enmascaramiento. (Pág. 4, Párr. 0070).
Presentar (416) anotaciones en una interfaz de usuario que indican cada una de las una o más porciones del contenido de usuario en la interfaz de usuario como que incluyen contenido confidencial, en donde las anotaciones están colocadas próximas a cada una de las una o más porciones y son seleccionables en la interfaz de usuario para presentar opciones de ofuscación.	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).

Resolución N° 37956

Ref. Expediente N° NC2019/0009852

	<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> (Hoja 7, Fig. 5). 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). (...) el método de enmascaramiento seleccionado para reemplazar los datos confidenciales con datos ficticios con fines de almacenamiento o presentación (...). (Pág. 3, Párr. 0056).	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														
En respuesta a seleccionar una primera de las anotaciones, presentar, en la interfaz de usuario, elementos de selección grafica que corresponden a las anotaciones e indican primeras opciones de ofuscación para reemplazar contenido confidencial asociado; 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 dentro de la interfaz de usuario de al menos una de las primeras opciones de ofuscación, reemplazar (418) al menos el contenido confidencial asociado con contenido ofuscado que mantiene un esquema de datos de al menos el contenido confidencial 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 17 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 18: 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

Resolución N° 37956

Ref. Expediente N° NC2019/0009852

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).

- Reivindicación 19: 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 20: 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 enmascaramiento se completaron con éxito para todos los archivos y (3) no se realizaron excepciones fatal.

Resolución N° 37956

Ref. Expediente N° NC2019/0009852

(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 18 a 20 tampoco cumplen con el requisito de novedad.

Respuesta a los argumentos del solicitante

El solicitante argumenta que “(...) *Las reivindicaciones 1, 9 y 17, en contraste con lo divulgado en el documento D1, se refieren a procesos particulares de ocultamiento de datos dentro de una aplicación y una interfaz gráfica de usuario para dicha aplicación. Específicamente, antes de ocultar el contenido sensible, la invención de la presente solicitud requiere presentar anotaciones gráficas en la interfaz de usuario para los datos sensibles detectados y proporciona elementos de selección gráfica en la interfaz de usuario para cada una de las anotaciones. Por tanto, un usuario puede entonces seleccionar entre los elementos de selección gráfica para realizar una o más operaciones de ofuscación para el contenido marcado en la interfaz de usuario con las anotaciones antes de enmascarar el contenido sensible (...) sin las indicaciones gráficas de interfaz de usuario que permite seleccionar características de ofuscamiento por parte del usuario (...)*”.

Se aclara que, contrario a lo afirmado por el solicitante, el documento D1 sí permite anticipar dichas características porque menciona: “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) y “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). De acuerdo con los párrafos anteriores se puede apreciar que el documento D1 anticipa la característica referente a la selección de alguna operación de ofuscación, particularmente en la selección de dicho método de enmascaramiento para preservar la confidencialidad de los datos.

El solicitante afirma que: “(...) Aunque el examinador, de acuerdo con el Oficio No 2, considera que la característica de “antes de ocultar el contenido confidencial, presentar (416) anotaciones gráficas visibles en una interfaz de usuario a la aplicación de usuario

Resolución N° 37956

Ref. Expediente N° NC2019/0009852

que anotan cada una de las una o más porciones del contenido de usuario en la interfaz de usuario como que incluyen contenido confidencial” está divulgado por los párrafos [0045], [0059], [0068] y [0070] del documento D1, dichos párrafos no divulgan dicha característica por las siguientes razones: - La visualización en pantalla de la que trata el párrafo [0059] del documento D1 es la visualización de reportes incluidos en una salida 115 después de ocultar el contenido y no lo hace antes de ocultar el contenido confidencial, como lo requiere la invención de la presente solicitud. El mismo documento D1, en su párrafo [0057], nombra a dicha salida 115 como una salida del proceso de enmascaramiento de datos, es decir que es una salida producto de dicho proceso de enmascaramiento y, por lo tanto, que se produce después del ocultamiento del contenido. El flujo de datos que se muestra en la figura 1 del documento D1 también muestra que la salida 115 se produce después del enmascaramiento (es decir, después del ocultamiento de información) (...) - Aunque el párrafo [0070] del documento D1 divulga que en un escenario en el que los datos provisionales (interim data, 318) existían antes de que se enmascararan los datos de origen (314), dicha existencia de los datos provisionales no corresponde a una presentación, y mucho menos a una presentación de anotaciones gráficas visibles en una interfaz de usuario. Por lo tanto, el párrafo [0070] del documento D1 no divulga ni sugiere la característica en cuestión (...).

Sin embargo, contrario a lo afirmado por el solicitante, dichos párrafos si permiten anticipar cada una de las características porque mencionan: “(...) Los datos provisionales (318) son datos que pueden ser de entrada y salida (...) En un escenario en el que los datos provisionales (318) existían antes de que se enmascararan los datos de origen 314, dichos datos provisionales deben considerarse candidatos para el enmascaramiento (...)” (Párr. 0070). De acuerdo con el párrafo anterior se puede evidenciar que el documento D1 toma en consideración datos antes de ocultar o enmascarar. Ahora bien, el documento D1 también menciona “(...) 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. 2, Párr. 0045), “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) y “(...) 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). De acuerdo con los párrafos anteriores, es posible evidenciar que dicha característica referida a la presentación de anotaciones gráficas previo a ocultar el contenido confidencial, es anticipada particularmente en el párrafo 0059 del documento D1 a partir de los informes de salida, y a las clasificaciones de contenido confidencial, mediante las clasificaciones de sensibilidad de datos divulgadas en D1, particularmente indicadas en el párrafo 0045.

El solicitante manifiesta que “(...) - El párrafo [0045] del documento D1 hace referencia a la Figura 5 del documento D1, en donde dicho párrafo y dicha figura muestra los tipos de clasificación de sensibilidad datos, pero no se refiere a indicaciones **visibles** presentadas en una interfaz de usuario como lo requiere la invención de la presente solicitud. Por lo tanto, el párrafo [0045] del documento D1 no divulga ni sugiere la característica en cuestión. - Aunque el párrafo [0068] del documento D1 divulga la introducción de datos fuente 314 en una interfaz en tiempo real, nada en el documento D1 divulga o sugiere que dicha introducción en tiempo real implique anotaciones gráficas visibles en la interfaz de usuario. Inclusive si se concluyera que la introducción de datos en tiempo real divulgado



Resolución N° 37956

Ref. Expediente N° NC2019/0009852

en el párrafo [0068] del documento D1 implica anotaciones gráficas visibles, que, como se evidencia a lo largo del documento D1, no lo hace, el documento D1 tampoco divulga o sugiere específicamente que dicha introducción en tiempo real implique anotaciones de que una o más porciones del contenido de usuario en la interfaz de usuario incluyen contenido confidencial como lo requiere la presente solicitud (...)

En importante destacar que, el documento D1 si permite anticipar la característica en referencia a las indicaciones de visualización porque menciona: “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). De acuerdo con el párrafo anterior, dichos informes incluidos en la salida de D1 permiten anticipar las indicaciones de visualización. Ahora bien, de igual manera resulta importante señalar que, de acuerdo con las modificaciones al pliego reivindicatorio allegadas bajo el radicado N° NC2019/0009852 del 25 de marzo de 2022, la característica de “tiempo real” no se encuentra de manera particular en las mismas, y por lo tanto no es objeto de estudio en el presente estudio de patentabilidad.

El solicitante sostiene que: “(...) Aunque el examinador, de acuerdo con el Oficio No 2, considera que la característica de “presentar, en la interfaz de usuario (112), elementos de selección grafica que corresponden a las anotaciones gráficas e indican opciones de ofuscación para ocultar el contenido confidencial” está divulgado por los párrafos [0006], [0053], [0056] y [0058] del documento D1, dichos párrafos no divulgan dicha característica por las siguientes razones: - Aunque el párrafo [0006] del documento D1 divulga la selección de 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, para dicha selección, el párrafo [0006] del documento D1 no menciona elementos de selección gráfica y mucho menos que dichos elementos de selección grafica correspondan a las anotaciones gráficas presentada en la interfaz de usuario. Nótese que la selección de un método de enmascaramiento no implica necesariamente elementos de selección grafica. - El párrafo [0053] y la Figura 13 del documento D1 se refieren a una tabla de normalizaciones ejemplares en donde dicha tabla de normalizaciones ejemplares no está relacionada con la presentación de elementos de selección gráfica y, por lo tanto, el párrafo [0053] o la Figura 13 divulgan la característica en cuestión. - El párrafo [0056] del documento D1 se refiere a los actores que pueden operar en los datos entregados en donde dichos actores no están relacionados con la presentación de elementos de selección gráfica y, por lo tanto, el párrafo [0056] no divulgan la característica en cuestión. - El párrafo [0058] del documento D1 divulga archivos de datos de preofuscación que incluyen elementos de datos pre enmascarados, es decir, datos que se ingresan a la aplicación comercial y que debe enmascarse para preservar la confidencialidad de los datos, en donde dichos archivos no están relacionados con la presentación de elementos de selección gráfica y, por lo tanto, no divulgan la característica en cuestión. (...)”

Contrario a lo afirmado por el solicitante, dichos párrafo si permiten anticipar la característica técnica esencial asociada porque mencionan: “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



Resolución N° 37956

Ref. Expediente N° NC2019/0009852

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) y “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). De acuerdo con los párrafos anteriores, se puede evidenciar que la característica de selección del método de ofuscación de la solicitud, es anticipada mediante el enmascaramiento, explícitamente mencionado en el párrafo 0006 del documento D1. Ahora bien, es importante destacar que, el hecho de que dicha selección no sea gráfica, no evita que se anticipe el efecto técnico asociado de dicha selección, y por lo tanto la materia reclamada en la característica técnica esencial, se encuentra anticipada por las enseñanzas del documento D1.

El solicitante menciona que: *“(…) Aunque el examinador, de acuerdo con el Oficio No 2, considera que la característica de “en respuesta a una selección de usuario dentro de la interfaz de usuario de al menos una de las opciones de ofuscación en un elemento de selección gráfica para contenido de usuario asociado, reemplazar (418) al menos el contenido de usuario asociado con contenido ofuscado que mantiene un esquema de datos de al menos el contenido de usuario asociado” está divulgado por los párrafos [0056] y [0117] del documento D1, dichos párrafos no divulgan dicha característica por las siguientes razones: - Aunque el párrafo [0056] del documento D1 divulga la ejecución de un método de enmascaramiento seleccionado para reemplazar los datos sensibles con datos ficticios para fines de almacenamiento o presentación, dicha ejecución del método de enmascaramiento divulgado en D1 no se realiza en respuesta a una selección de usuario dentro de la interfaz de usuario como se requiere en la invención de la presente solicitud y, por lo tanto, no divulgan la característica en referencia. - Aunque el párrafo [0117] del documento D1 divulga un remplazo universal de una instancia del valor pre-enmascarado con un valor post-enmascarado, dicho remplazo divulgado en el documento D1 no se realiza en respuesta a una selección de usuario dentro de la interfaz de usuario como se requiere en la invención de la presente solicitud y, por lo tanto, no divulgan la característica en referencia (…)”*

Se aclara que no es así porque, porque el documento D1 menciona: *“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) y “Una regla (también conocida como regla de remplazo 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 remplazo 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 los párrafos anteriores, es posible evidenciar que dicha etapa de selección sí esta anticipada, particularmente en el párrafo 0056 del documento D1, a partir del método de enmascaramiento seleccionado. Aunado a lo anterior, el párrafo 0117 relaciona que pueden existir diferentes reglas de remplazo, que al ser seleccionadas permiten pasar un enmascaramiento inicial a otro posterior o final, por lo que se mantienen las objeciones por novedad.*

El solicitante asegura que: *“(…) Aunque el examinador, de acuerdo con el Oficio No 2, considera que la característica de “proporcionar contenido de usuario que comprende un archivo de datos de usuario visible en la aplicación de usuario a un servicio de clasificación” está divulgado por los párrafos [0059] y [0068] del documento D1, dichos párrafos no divulgan dicha característica por las siguientes razones: - La visualización en*

Resolución N° 37956

Ref. Expediente N° NC2019/0009852

pantalla de la que trata el párrafo [0059] del documento D1 corresponde a una visualización de reportes incluidos en una salida 115 y no a una visualización de un archivo de datos de usuario como lo requiere la solicitud de la presente solicitud. El reporte de la salida 115 corresponde a reportes de un repositorio de captura de auditoría 116, de un repositorio de informes y datos de control de validación, y archivos de datos dentro del alcance posteriores a la ofuscación (ver documento D1, párrafo [0057]) y por, lo tanto, nada en el documento D1 indica que dicho reporte corresponda a un archivo de datos de usuario, y en conclusión la característica es cuestión no está divulgada por el párrafo [0059] del documento D1. El mismo documento D1 en su párrafo [0142], indica que el reporte de captura de auditoría de la salida 115 sirve como una auditoría para registrar la acción realizada en los datos, y, por lo tanto, no contiene datos de usuario. - Aunque el párrafo [0068] del documento D1 divulga la introducción de datos fuente 314 en una interfaz en tiempo real, nada en el documento D1 divulga o sugiere que dichos datos fuente 314 sean datos de usuario, y en conclusión la característica es cuestión no está divulgada por el párrafo [0068] del documento D1 (...)

Contrario a lo afirmado por el solicitante, dichos párrafos si permiten anticipar la característica técnica mencionada por que indican, en primer lugar que: “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) y “Los datos de origen (314) de la aplicación externa (310) se introducen en la aplicación (302) (...)” (Pág. 4, Párr. 0068). De acuerdo con los párrafos anteriores se puede evidenciar que dicha característica referida a proporcionar contenido en una aplicación de usuario es anticipada por la materia referida a los informes de salida y la aplicación externa indicadas en D1. Ahora bien, es segundo lugar el documento D1 también menciona: “(...) un servicio de soporte (...)” (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) y “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). De acuerdo con los párrafos anteriores, se puede apreciar que dicho servicio de clasificación para procesar el contenido de usuario en porciones del contenido confidencial o esquemas de datos predeterminados es anticipado por el servicio de soporte indicado en el párrafo 0008 y la clasificación de datos sensibles en categorías, particularmente mencionados en el párrafo 0018 del documento D1.

El solicitante indica que: “(...) Por lo tanto, no hay ninguna enseñanza o sugerencia en el documento D1 de “presentar anotaciones gráficas” que presenta los datos con anotaciones antes de ocultar los datos. Además, no hay ninguna enseñanza o sugerencia en el documento D1 de proporcionar elementos de selección gráfica en la interfaz de usuario para cada una de dichas anotaciones, donde esos elementos de selección gráfica pueden ser seleccionados por un usuario y utilizados para iniciar el ocultamiento de los datos. (...)”

Se reitera al solicitante que dichas características sí son anticipadas por el documento D1 porque menciona: “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



Resolución N° 37956

Ref. Expediente N° NC2019/0009852

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) y “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). En los párrafos anteriores se evidencia que a partir de los informes de salida o la aplicación externa mencionados en D1 se puede anticipar dicha característica referida a la presentación de anotaciones gráficas. De igual manera, el documento D1 menciona: “Los datos provisionales (318) son datos que pueden ser de entrada y salida (...) En un escenario en el que los datos provisionales (318) existían antes de que se enmascararan los datos de origen (314), dichos datos provisionales deben considerarse candidatos para el enmascaramiento” (Párr. 0070). De acuerdo con el párrafo 0070 del documento D1, se puede evidenciar que dicha anticipación a la ocultación de los datos es divulgada por aquellos datos existentes antes del enmascaramiento en D1. Finalmente, la selección de datos utilizados por un usuario y utilizados para iniciar el ocultamiento también es anticipada por D1 porque indica: “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) y “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). De acuerdo con los párrafos anteriores dicha selección se anticipa explícitamente en el documento D1 particularmente en el párrafo 0006 y se puede realizar a través de la aplicación comercial indicada en el párrafo 0058.

Por último, realiza la petición consistente en que “(...) me permito solicitar a ese Despacho, proceder con la revisión de las modificaciones y de los argumentos aquí presentados, para conceder el privilegio de patente solicitado para la materia objeto de las 20 reivindicaciones ahora presentadas en el capítulo reivindicatorio modificado, y que de subsistir alguna duda o inquietud respecto a la patentabilidad de la presente invención, a pesar de las modificaciones y argumentos técnicos ahora presentados, sin apartarse del espíritu inventivo originalmente revelado en la solicitud internacional, se le brinde la oportunidad al solicitante de aclararla o de limitar aún más la invención, mediante la emisión de un segundo examen de fondo, teniendo en cuenta el nuevo capítulo reivindicatorio que se somete a revisión, antes de que se emita una decisión definitiva por parte de este despacho, de conformidad con lo dispuesto en 1.2.2.5.1. del artículo primero de la Resolución 54093 de 2012 (...) en el evento que el examinador considere que pese a las modificaciones presentadas aún existen objeciones, que proceda a emitir un segundo examen de fondo sobre el nuevo capítulo presentado” y sobre esta solicitud la Oficina aclara que ya se han realizado dos exámenes de patentabilidad de la presente solicitud notificándole los Oficios N° 11103 del 14 de julio de 2021 y el Oficio N° 2 del 3 de enero de 2022, ante los cuales el solicitante ya tuvo la oportunidad de exponer sus argumentos, por lo que no considera necesario realizar un tercer examen de patentabilidad teniendo en cuenta que no se presentó una modificación sustancial del capítulo reivindicatorio, ni se acreditó el pago de la tasa correspondiente a un nuevo examen de patentabilidad. Además, es importante precisar que la circular única fue modificada a finales del año 2021 en lo referente al citado numeral.



Resolución N° 37956

Ref. Expediente N° NC2019/0009852

Que de acuerdo con la modificación presentada por el solicitante en el escrito radicado bajo el N° NC2019/0009852 el 5 de octubre de 2021 y teniendo en cuenta el objeto de la solicitud, se modifica el título de la invención el cual quedará de la siguiente manera: “MÉTODOS Y ESTRUCTURA DE OFUSCACIÓN DEL CONTENIDO DE USUARIO EN ARCHIVOS DE DATOS ESTRUCTURADOS DE USUARIO”.

En conclusión, teniendo en cuenta que los argumentos del solicitante no desvirtúan de manera alguna las objeciones a la patentabilidad ya sustentadas, el Superintendente de Industria y Comercio,

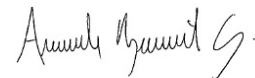
RESUELVE

ARTÍCULO 1: Denegar la patente de invención a la creación titulada “MÉTODOS Y ESTRUCTURA DE OFUSCACIÓN DEL CONTENIDO DE USUARIO EN ARCHIVOS DE DATOS ESTRUCTURADOS DE USUARIO”.

ARTÍCULO 2: Notificar el contenido de la presente resolución a LLC MICROSOFT TECHNOLOGY LICENSING, advirtiéndole que contra ella procede el recurso de reposición, ante el Superintendente de Industria y Comercio, el cual podrá ser interpuesto en el momento de la notificación o dentro de los diez (10) días hábiles siguientes a ella

NOTIFÍQUESE Y CÚMPLASE

Dada en Bogotá D.C., el 16 de junio de 2022



ANDRÉS BARRETO GONZÁLEZ
SUPERINTENDENTE DE INDUSTRIA Y COMERCIO

Firmado digitalmente
por: ANDRÉS
BERNARDO BARRETO
GONZÁLEZ
Fecha: 2022.06.16
17:01:20 COT
Razón: Validez jurídica.
Ubicación: Bogotá,
Colombia.