

REPÚBLICA DE COLOMBIA
SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO

Resolución N° 70158

Ref. Expediente N° NC2020/0001367

Por la cual se deniega una Patente de Modelo de Utilidad

LA DIRECTORA DE NUEVAS CREACIONES

en ejercicio de sus facultades legales, en especial de las conferidas en el numeral 5° del artículo 20 del Decreto 4886 de 2011, y

CONSIDERANDO

PRIMERO: Que mediante escrito radicado en esta Superintendencia el 7 de febrero de 2020 con el N° NC2020/0001367, por CONTROLES INTELIGENTES SAS, presentó la solicitud de patente de modelo de utilidad titulada “MECANISMO PARA LA IDENTIFICACIÓN, VALIDACION DE LOS REQUERIMIENTOS DE SEGURIDAD Y ELEMENTOS DE PROTECCIÓN PERSONAL POR PARTE DEL TRABAJADOR PARA REALIZAR LABORES DETERMINADAS EN LA EMPRESA”.

SEGUNDO: Que la solicitud fue publicada en la Gaceta de la Propiedad Industrial N° 886 el 18 de febrero de 2020, sin que se hubieran presentado oposiciones por parte de terceros.

TERCERO: Que realizado el examen de fondo mediante Oficio N° 10866, notificado el 01 de septiembre de 2020, se requirió a la 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.

CUARTO: Que el solicitante mediante escrito radicado bajo el N° NC2020/0001367 el 13 de octubre de 2020, respondió oportunamente el requerimiento formulado sin presentar nuevo capítulo reivindicatorio. Por lo tanto, se tendrá en cuenta el capítulo reivindicatorio presentado con el radicado N° NC2020/0001367 el 02 de agosto de 2020.

QUINTO: Teniendo en cuenta lo dispuesto en el artículo 85 de la Decisión 486 expedida por la Comisión de la Comunidad Andina *“Son aplicables a las patentes de modelo de utilidad, las disposiciones sobre patentes de invención contenidas en la presente Decisión en lo que fuere pertinente, salvo en lo dispuesto con relación a los plazos de tramitación, los cuales se reducirán a la mitad. Sin perjuicio de lo anterior, el plazo establecido en el artículo 40 quedará reducido a doce meses.”*

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”.*

Resolución N° 70158

Ref. Expediente N° NC2020/0001367

Asimismo, el artículo 81 de la Decisión 486 indica “Se considera modelo de utilidad, a toda nueva forma, configuración o disposición de elementos, de algún artefacto, herramienta, instrumento, mecanismo u otro objeto o de alguna parte del mismo, que permita un mejor o diferente funcionamiento, utilización o fabricación del objeto que le incorpore o que le proporcione alguna utilidad, ventaja o efecto técnico que antes no tenía. Los modelos de utilidad se protegerán mediante patentes”.

SEXTO: Que en el presente caso las reivindicaciones 1 a 4 incluidas en el radicado bajo el N° NC2020/0001367 el 13 de octubre de 2020, no cumplen los requisitos indicados. Lo anterior, de acuerdo con las siguientes consideraciones:

6.1 Objeto de la invención

El problema planteado consiste en la necesidad de suministrar un mecanismo para comprobar que el trabajador de una empresa cuente con los requerimientos de seguridad, logrando así mejorar la seguridad en el trabajo y salvaguardar la responsabilidad del empleador por posibles siniestros.

Para resolver este problema técnico, se proporciona un mecanismo que por medio de controladoras de validación, dispositivos de almacenamiento, mecanismos de identificación y dispositivos de autenticación, por ejemplo: huellas dactilares, lector de tarjeta con o sin contacto, lector de código de barras, teclado físico, pantalla táctil, lector de iris, cámara para reconocimiento facial, entre otros; permiten almacenar y procesar información del trabajador, para comprobar que el trabajador cuenta con requerimientos de seguridad comprendidos por: elementos de protección personal, capacitaciones y certificaciones para realizar una labor.

6.2 Determinación del estado de la técnica

La fecha para determinar el estado de la técnica es el 07 de febrero de 2020, que corresponde a la fecha de presentación nacional.

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
D2	WO 2017/155968	“Intelligent Safety Monitoring And Analytics System For Personal Protective Equipment”	14 de septiembre de 2017

El documento D2¹ divulga técnicas y sistemas que brindan monitoreo y análisis inteligente para los trabajadores y los datos del equipo de protección personal en relación con los entornos de trabajo basados en datos históricos y en tiempo real (Pág. 1, Párr. 005).

¹https://worldwide.espacenet.com/publicationDetails/description?CC=WO&NR=2017155968A1&KC=A1&FT=D&ND=3&date=20170914&DB=&locale=en_EP

Resolución N° 70158

Ref. Expediente N° NC2020/0001367

6.3 Novedad

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 mecanismo reclamado en la solicitud no es nuevo, teniendo en cuenta que la reivindicación 1 está referida a: *“MECANISMO PARA LA IDENTIFICACIÓN, VALIDACIÓN DE LOS REQUERIMIENTOS (...)”* (Radicado N° NC2020/0001367 del 02 de agosto de 2020).

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	D2
MECANISMO PARA LA IDENTIFICACIÓN, VALIDACION DE LOS REQUERIMIENTOS DE SEGURIDAD Y ELEMENTOS DE PROTECCION PERSONAL POR PARTE (...)	Esta divulgación está dirigida a técnicas y sistemas que brindan monitoreo y análisis inteligente para los trabajadores y los datos del equipo de protección personal en relación con los entornos de trabajo basados en datos históricos y en tiempo real (Pág. 1, Párr. 005).
Uno a más dispositivos de identificación (1) que identifica al trabajador, los cuales está conectado o comunicado con una o más controladoras de validación (5).	Por ejemplo, el lugar de trabajo (110) puede incluir uno o más lectores, balizas u otros dispositivos informáticos que pueden detectar la credencial del trabajador, el dispositivo informático portátil (114A) o cualquier otro dispositivo de identificación. Alternativamente, el dispositivo informático portátil (114A) puede detectar los lectores, balizas u otros dispositivos informáticos (Pág. 8, Párr. 049). Como se muestra en la figura 2, la aplicación (228) se ejecuta en el espacio de usuario (202) del dispositivo informático (200). La aplicación (228) se puede dividir lógicamente en la capa de presentación (222), la capa de aplicación (224) y la capa de datos (226). La capa de presentación (222) puede incluir el componente (228) de interfaz de usuario (UI), que genera y representa interfaces de usuario de la aplicación (228), tales como interfaces de usuario ilustradas en las FIGS. 3-20. La capa de aplicación (224) puede incluir el componente de recomendación (230), el componente de supervisión (232), el componente de alerta (234) y el componente de registro (236). El componente de registro (236) puede recibir varios datos de los dispositivos informáticos del lugar de trabajo (por ejemplo, el dispositivo informático (104) del lugar de trabajo de la figura 1A), dispositivos informáticos portátiles (114) y/o cualquier otro dispositivo informático. El componente de registro (236) puede

Resolución N° 70158

Ref. Expediente N° NC2020/0001367

	almacenar los datos en uno o más almacenes de datos que comprenden datos, tales como, entre otros, datos de trabajador (238), datos de equipo (240), datos de lugar de trabajo (242), datos de actividad (244) y/o cualquier otro dato (Pág. 19 a Pág. 20, Párr. 084).
Uno o más dispositivos de autenticación (4) que valida el uso de los elementos de protección personal y/o dotación requeridos, los cuales están conectados o comunicados con la controladora de validación (5).	En algunos ejemplos, el componente de monitoreo (232) puede generar una puntuación de riesgo basada en uno o más parámetros, tales como, entre otros: exposición del trabajador a peligros en el ambiente de trabajo, uso de equipo de protección personal por parte del trabajador, tiempo de trabajo en el ambiente de trabajo, o cualquier otro parámetro que indique riesgo para el usuario (Pág. 22, Párr. 091). El componente de registro (236) puede recibir varios datos de los dispositivos informáticos del lugar de trabajo (por ejemplo, el dispositivo informático (104) del lugar de trabajo de la figura 1A), los dispositivos informáticos portátiles (114) y/o cualquier otro dispositivo informático. El componente de registro (236) puede almacenar los datos en uno o más almacenes de datos que comprenden datos, tales como, pero sin limitarse a: datos de trabajador (238), datos de equipo (240), datos de lugar de trabajo (242), datos de actividad (244) y/o cualquier otro dato (Pág. 19 a 20, Párr. 084).
Una o más controladoras de validación (5) que están conectadas o comunicadas con uno o más dispositivos de identificación (1), uno o más dispositivos autenticación (4), uno o más dispositivos almacenamiento (3).	Por ejemplo, el lugar de trabajo (110) puede incluir uno o más lectores, balizas u otros dispositivos informáticos que pueden detectar la credencial del trabajador, el dispositivo informático portátil (114A) o cualquier otro dispositivo de identificación. Alternativamente, el dispositivo informático portátil (114A) puede detectar los lectores, balizas u otros dispositivos informáticos (Pág. 8, Párr. 049). El componente de registro (236) puede recibir varios datos de los dispositivos informáticos del lugar de trabajo (por ejemplo, el dispositivo informático (104) del lugar de trabajo de la figura 1A), los dispositivos informáticos portátiles (114) y/o cualquier otro dispositivo informático. El componente de registro (236) puede almacenar los datos en uno o más almacenes de datos que comprenden datos, tales como, pero sin limitarse a: datos de trabajador (238), datos de equipo (240), datos de lugar de trabajo (242), datos de actividad (244) y/o cualquier otro dato (Pág. 19 a 20, Párr. 084).
Uno o más dispositivos de almacenamiento (3) que se encarga de almacenar la información del trabajador, los elementos de protección personal requeridos por el trabajador, la entrega de la dotación por parte del empleador y las certificaciones y capacitaciones, los cuales están conectados o comunicados a una o más controladoras de validación (5).	El componente de registro (236) puede recibir varios datos de los dispositivos informáticos del lugar de trabajo (por ejemplo, el dispositivo informático (104) del lugar de trabajo de la figura 1A), los dispositivos informáticos portátiles (114) y/o cualquier otro dispositivo informático. El componente de registro (236) puede almacenar los datos en uno o más almacenes de datos que comprenden datos, tales como, pero sin limitarse a: datos de trabajador (238), datos de equipo (240), datos de lugar de trabajo (242), datos de actividad (244) y/o cualquier otro dato (Pág. 19 a 20, Párr. 084). Los datos (240) del equipo pueden incluir información de identificación del equipo, como por ejemplo, pero no limitado a: identificador único del equipo, especificaciones del equipo,

Resolución N° 70158

Ref. Expediente N° NC2020/0001367

	clasificaciones de ruido o cualquier otro dato relacionado con un equipo. Los datos del lugar de trabajo (242) pueden incluir información del lugar de trabajo, como, entre otros, el identificador único del lugar de trabajo, la ubicación del lugar de trabajo, las condiciones de trabajo del lugar de trabajo (por ejemplo, peligros, niveles de ruido, clima, por nombrar solo algunos ejemplos). Los datos de actividad (244) pueden incluir información de actividad que indique una instancia particular de datos de lugar de trabajo, trabajadores y equipos (Pág. 22, Párr. 085).
Una unidad de almacenamiento (10) para almacenar información de firmas electrónicas (8) es diferente al dispositivo de almacenamiento (3).	En algunos ejemplos, los datos de los trabajadores (238) pueden incluir información biométrica sobre los trabajadores, que incluye, entre otros, la temperatura corporal, la frecuencia cardíaca o cualquier otra medida biométrica (Pág. 20, Párr. 085). Cabe aclarar que el capítulo descriptivo inicial de la solicitud menciona que la firma electrónica puede corresponder a información biométrica. Los almacenes de datos para datos de trabajadores (238), datos de equipo (240), datos de lugar de trabajo (242), datos de actividad (244) pueden ser uno o más de un sistema de gestión de base de datos relacional, base de datos de procesamiento analítico en línea, tabla o cualquier otra estructura adecuada para almacenar datos (Pág. 20, Párr. 084). Los dispositivos de almacenamiento (212), en algunos ejemplos, también incluyen uno o más medios de almacenamiento legibles por ordenador. Los dispositivos de almacenamiento (212) pueden configurarse para almacenar mayores cantidades de información que la memoria volátil. Los dispositivos de almacenamiento (212) pueden configurarse además para el almacenamiento a largo plazo de información como espacio de memoria no volátil y retener información después de los ciclos de activación/desactivación (Pág. 19, Párr. 083).
Una o más Interfaz de usuario (6) conectado o comunicado con una o más controladoras de validación (5).	Como se muestra en la figura 2, la aplicación (228) se ejecuta en el espacio de usuario (202) del dispositivo informático (200). La aplicación (228) se puede dividir lógicamente en la capa de presentación (222), la capa de aplicación (224) y la capa de datos (226). La capa de presentación (222) puede incluir el componente (228) de interfaz de usuario (UI), que genera y representa interfaces de usuario de la aplicación (228) (Pág. 19, Párr. 084).
Un módulo GPS (9) que permite identificar la ubicación donde el trabajador solicita la autorización y está conectado con la controladora de validación.	Un dispositivo informático portátil usado o asociado de otro modo con el trabajador puede enviar datos de ubicación al dispositivo informático (200), que se almacena mediante el componente de monitoreo (232) en los datos del trabajador (238). Los datos de ubicación pueden ser coordenadas GPS u otros identificadores de ubicaciones dentro de un entorno de trabajo, como como, pero no limitado a, un identificador de baliza en una ubicación particular u otra ubicación relativa (Pág. 29, Párr. 106).

Resolución N° 70158

Ref. Expediente N° NC2020/0001367

De acuerdo con la tabla anterior, las características esenciales del mecanismo 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 3: Los componentes de entrada (242) del dispositivo informático (200), en un ejemplo, incluyen un ratón, teclado, sistema de respuesta por voz, cámara de vídeo, botones, panel de control, micrófono o cualquier otro tipo de dispositivo para detectar la entrada de una persona o una máquina. En algunos ejemplos, el componente de entrada (242) puede ser un componente de entrada sensible a la presencia, que puede incluir una pantalla sensible a la presencia, una pantalla sensible al tacto, etc. (Pág. 18, Párr. 079).
- Reivindicación 4: En algunos ejemplos, los datos de los trabajadores (238) pueden incluir información biométrica sobre los trabajadores, que incluye, entre otros, la temperatura corporal, la frecuencia cardíaca o cualquier otra medida biométrica (Pág. 20, Párr. 085). Los componentes de entrada (242) del dispositivo informático (200), en un ejemplo, incluyen un ratón, teclado, sistema de respuesta por voz, cámara de vídeo, botones, panel de control, micrófono o cualquier otro tipo de dispositivo para detectar la entrada de una persona o una máquina. En algunos ejemplos, el componente de entrada (242) puede ser un componente de entrada sensible a la presencia, que puede incluir una pantalla sensible a la presencia, una pantalla sensible al tacto, etc. (Pág. 18, Párr. 079).

Las reivindicaciones dependientes 3 y 4 tampoco cumplen con el requisito de novedad.

6.4 Respuesta a los argumentos del solicitante

El solicitante afirma que “(...) El documento D2 está diseñado para monitorear y analizar los niveles de ruido en los entornos de trabajo. No contempla la validación del uso de los elementos de protección personal por parte del trabajador, ni mucho menos del cumplimiento de los requerimientos de seguridad (...)”.

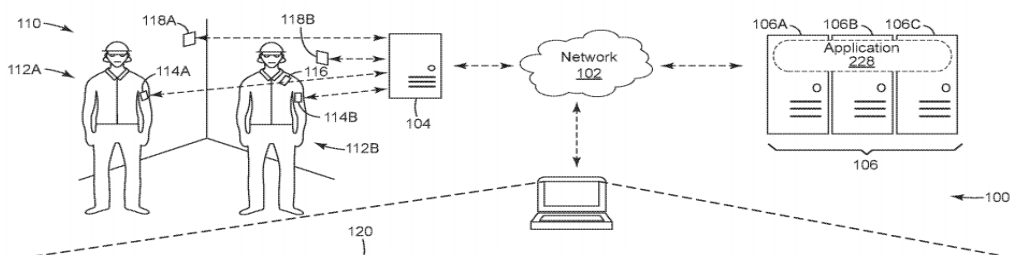
Al respecto, resulta conveniente aclarar que el documento D2 corresponde al campo técnico de la invención al divulgar técnicas y sistemas que brindan monitoreo y análisis inteligente para los trabajadores y los datos del equipo de protección personal en relación con los entornos de trabajo basados en datos históricos y en tiempo real (Pág. 1, Párr. 005). Por lo tanto, este documento se refiere al análisis de datos de equipo de protección de los trabajadores y por ende de los requerimientos de seguridad que debe cumplir una empresa determinada de acuerdo con la evaluación de esta información, por lo que este argumento no resulta procedente para desvirtuar la utilización de este documento en el análisis de novedad realizado.



Resolución N° 70158

Ref. Expediente N° NC2020/0001367

Por otro lado, en referencia al argumento del solicitante, según el cual afirma que “(...) El examinador identifica ‘lectores, balizas u otros dispositivos informáticos’ como los dispositivos de identificación. El examinador identifica ‘el dispositivo informático portátil (114A)’ como la controladora de validación (...)”, es pertinente indicar que contrario a lo afirmado por el solicitante, el dispositivo (114A) se ha reconocido como el dispositivo de identificación al mencionar el documento D2 que el lugar de trabajo (110) puede incluir uno o más lectores, balizas u otros dispositivos informáticos que pueden detectar la credencial del trabajador, el dispositivo informático portátil (114A) o cualquier otro dispositivo de identificación. Alternativamente, el dispositivo informático portátil (114A) puede detectar los lectores, balizas u otros dispositivos informáticos (Pág. 8, Párr. 049). Adicionalmente, como se observa en la siguiente figura, se puede apreciar que los dispositivos (114A) son portados por cada trabajador en particular con la finalidad de enviar datos de identificación de cada uno:



(Pág. 74, Fig. 1A).

Sumado a lo anterior, el dispositivo informático (200) se ha reconocido como la controladora de validación, al referirse el documento D2 que la aplicación (228) se ejecuta en el espacio de usuario (202) del dispositivo informático (200). La aplicación (228) se puede dividir lógicamente en la capa de presentación (222), la capa de aplicación (224) y la capa de datos (226). La capa de presentación (222) puede incluir el componente (228) de interfaz de usuario (UI), que genera y representa interfaces de usuario de la aplicación (228), tales como interfaces de usuario ilustradas en las FIGS. 3-20. La capa de aplicación (224) puede incluir el componente de recomendación (230), el componente de supervisión (232), el componente de alerta (234) y el componente de registro (236). El componente de registro (236) puede recibir varios datos de los dispositivos informáticos del lugar de trabajo (por ejemplo, el dispositivo informático (104) del lugar de trabajo de la figura 1A), dispositivos informáticos portátiles (114) y/o cualquier otro dispositivo informático. El componente de registro (236) puede almacenar los datos en uno o más almacenes de datos que comprenden datos, tales como, entre otros, datos de trabajador (238), datos de equipo (240), datos de lugar de trabajo (242), datos de actividad (244) y/o cualquier otro dato (Pág. 19 a Pág. 20, Párr. 084). En este párrafo se puede evidenciar que el componente de registro (236) que hace parte del dispositivo informático (200), recibe datos de los dispositivos informáticos portátiles (114A), es decir este dispositivo informático (200) recibe información correspondiente a los trabajadores por parte del dispositivo de identificación, lo cual implica que se encuentran conectados el uno con el otro, por lo cual esta característica es anticipada por el documento D2 tal como se evidencia en el análisis de novedad realizado.

Resolución N° 70158

Ref. Expediente N° NC2020/0001367

Ahora bien, respecto al argumento del solicitante que sostiene que “(...) Ninguna parte de la citación realizada por el examinador muestra un dispositivo de autenticación con las características definidas en la patente ‘Cuando hablamos de “dispositivos de autenticación” se hace referencia a componentes que tienen la capacidad de demostrar que un usuario es realmente quien asegura ser, lo que a su vez permite autenticar y validar la información que ingresa en el mecanismo. Ejemplo de estos componentes son: lector de huella, lector de tarjeta con o sin contacto, lector de código de barras, teclado físico, pantalla táctil, lector de iris, y/o cámara para reconocimiento facial, entre otros” (...), cabe aclarar que el capítulo reivindicatorio allegado bajo el No. NC2020/0001367 del 02 de agosto de 2020 no menciona de manera explícita que los dispositivos de autenticación son “componentes que tienen la capacidad de demostrar que un usuario es realmente quien asegura ser, lo que a su vez permite autenticar y validar la información que ingresa en el mecanismo”, por lo cual no hace parte del análisis de novedad realizado ni resulta válido para desvirtuar el mismo.

Por consiguiente, dado que la reivindicación independiente 1 menciona “(...) Uno o más dispositivos de autenticación (4) que valida el uso de los elementos de protección personal y/o dotación requeridos, los cuales están conectados o comunicados con la controladora de validación (5) (...)”, esto es anticipado por el documento D2 al referirse que el componente de monitoreo (232) puede generar una puntuación de riesgo basada en uno o más parámetros, tales como, entre otros: exposición del trabajador a peligros en el ambiente de trabajo, uso de equipo de protección personal por parte del trabajador, tiempo de trabajo en el ambiente de trabajo, o cualquier otro parámetro que indique riesgo para el usuario (Pág. 22, Párr. 091). El componente de registro (236) puede recibir varios datos de los dispositivos informáticos del lugar de trabajo (por ejemplo, el dispositivo informático (104) del lugar de trabajo de la figura 1A), los dispositivos informáticos portátiles (114) y/o cualquier otro dispositivo informático. El componente de registro (236) puede almacenar los datos en uno o más almacenes de datos que comprenden datos, tales como, pero sin limitarse a: datos de trabajador (238), datos de equipo (240), datos de lugar de trabajo (242), datos de actividad (244) y/o cualquier otro dato (Pág. 19 a 20, Párr. 084). En estos párrafos se puede evidenciar que el componente de monitoreo (232) que se comunica con los demás módulos de la controladora de validación (dispositivo informático (200)), genera una puntuación de riesgo basado en el uso de equipo de protección personal por parte del trabajador, es decir, valida el uso de elementos de protección personal y/o dotación requeridos, tal como lo realizan los dispositivos de autenticación de la reivindicación independiente 1, por lo cual esta característica es igualmente anticipada por el documento D2 y se mantienen las objeciones por novedad de acuerdo al artículo 16 de la Decisión 486.

Por otra parte, en relación con el argumento del solicitante que afirma que “(...) El mecanismo del documento D2 ni siquiera contempla la necesidad de autenticar transacciones ni documentos (...)”, resulta oportuno indicar que el capítulo reivindicatorio allegado bajo el No. NC2020/0001367 del 02 de agosto de 2020 no menciona de manera explícita esta característica, por lo tanto, no hace parte del estudio de patentabilidad realizado. Resulta del caso señalar que, el artículo 30 de la Decisión 486

Resolución N° 70158

Ref. Expediente N° NC2020/0001367

señala que las reivindicaciones deben ser claras y concisas y contener todas las características técnicas esenciales de la invención.

A continuación, el solicitante señala que *“(...) Adicionalmente el documento D2 no menciona explícitamente las firmas electrónicas tal y como están definidas en la invención (...)”*.

Al respecto, es pertinente aclarar que el capítulo descriptivo de la solicitud de la invención menciona respecto a las firmas electrónicas que *“(...) cuando se habla de “firma electrónica” se habla de métodos tales como, códigos, contraseñas, datos biométricos, o claves criptográficas privadas, que permite identificar a una persona dentro de una transacción de forma segura, la cual cuenta con una cadena de custodia y una unidad de almacenamiento de las firmas electrónicas y sus transacciones (...)”* (Pág. 3), es decir, un dato biométrico en particular puede corresponder a una firma electrónica. Por tanto, dado que la reivindicación independiente 1 recita *“Una unidad de almacenamiento (10) para almacenar información de firmas electrónicas (8) es diferente al dispositivo de almacenamiento (3)”*, esto es anticipado por el documento D2 al hacer mención que los datos de los trabajadores (238) pueden incluir información biométrica sobre los trabajadores, que incluye, entre otros, la temperatura corporal, la frecuencia cardíaca o cualquier otra medida biométrica (Pág. 20, Párr. 085). Los almacenes de datos para datos de trabajadores (238), datos de equipo (240), datos de lugar de trabajo (242), datos de actividad (244) pueden ser uno o más de un sistema de gestión de base de datos relacional, base de datos de procesamiento analítico en línea, tabla o cualquier otra estructura adecuada para almacenar datos (Pág. 20, Párr. 084). Los dispositivos de almacenamiento (212), en algunos ejemplos, también incluyen uno o más medios de almacenamiento legibles por ordenador. Los dispositivos de almacenamiento (212) pueden configurarse para almacenar mayores cantidades de información que la memoria volátil. Los dispositivos de almacenamiento (212) pueden configurarse además para el almacenamiento a largo plazo de información como espacio de memoria no volátil y retener información después de los ciclos de activación/desactivación (Pág. 19, Párr. 083). En estos párrafos se evidencia que la unidad de almacenamiento correspondiente al almacén datos de trabajadores, almacena datos tales como información biométrica de trabajadores, es decir la firma electrónica de los mismos, por lo que esta característica es igualmente anticipada por el documento D2 y se mantienen las objeciones por novedad.

Respecto al argumento del solicitante que menciona *“(...) En esta citación está identificando otro dispositivo “dispositivo informático (200)” el cual es completamente diferente al 114A. El dispositivo 114A no se encuentra conectado, ni comunicado con una interfaz de usuario. Por lo tanto el documento D2 no anticipa la interfaz de usuario conectada o comunicada con una o más controladoras de validación (...)”*, resulta conveniente aclarar que dado que el dispositivo informático (200) ha sido reconocido como la controladora de validación por las razones ya expuestas anteriormente, el documento D2 si anticipa la conexión de una interfaz de usuario a esta controladora al mencionar que la aplicación (228) se ejecuta en el espacio de usuario (202) del dispositivo informático (200). La aplicación (228) se puede dividir lógicamente en la capa

Resolución N° 70158

Ref. Expediente N° NC2020/0001367

de presentación (222), la capa de aplicación (224) y la capa de datos (226). La capa de presentación (222) puede incluir el componente (228) de interfaz de usuario (UI), que genera y representa interfaces de usuario de la aplicación (228) (Pág. 19, Párr. 084). Por ende, dado que la capa de presentación (222) se encuentra dentro del dispositivo informático (200), este está interconectado con la interfaz de usuario, por lo cual esta característica es divulgada por el documento D2 tal como se evidencia en el análisis de novedad realizado.

Ahora bien, en relación al argumento del solicitante que señala que “(...) *El dispositivo 114A no se encuentra conectado con un módulo GPS. Adicionalmente el dispositivo informático 200 no menciona explícitamente un módulo GPS. Por lo tanto el documento D2 no anticipa el modulo GPS conectado con la controladora de validación (...)*”, cabe indicar que el documento D2 hace referencia a que un dispositivo informático portátil usado o asociado de otro modo con el trabajador puede enviar datos de ubicación al dispositivo informático (200), que se almacena mediante el componente de monitoreo (232) en los datos del trabajador (238). Los datos de ubicación pueden ser coordenadas GPS u otros identificadores de ubicaciones dentro de un entorno de trabajo, como como, pero no limitado a, un identificador de baliza en una ubicación particular u otra ubicación relativa (Pág. 29, Párr. 106). En este párrafo se evidencia que el dispositivo informático portátil puede enviar datos de ubicación como coordenadas de GPS, es decir, este dispositivo cuenta con un módulo GPS que envía estos datos al dispositivo informático (200) que corresponde a la controladora de validación como ya fue explicado anteriormente. Por consiguiente, esta característica se anticipa por este documento y se mantienen las objeciones por novedad.

Por último, de acuerdo con el argumento del solicitante respecto a la reivindicación dependiente 2 “(...) *El examinador cita un proceso más no un mecanismo de control de acceso. Un proceso no puede anticipar un mecanismo de control de acceso. En ninguna parte del documento D2 se menciona explícitamente un dispositivo de control de acceso para restringir ingreso a una zona de trabajo o para activar el uso de una máquina. Este elemento no es anticipado por el documento D2 (...)*”, resulta oportuno aclarar que el documento D2 no menciona de manera explícita la utilización de dispositivos de control de acceso que permiten al trabajador el ingreso a una zona o activa el uso de una máquina y que están conectados o comunicados con una o más controladoras de validación, por lo tanto, esta objeción se entiende por superada.

En conclusión, teniendo en cuenta que los argumentos de la solicitante no desvirtúan de manera alguna las objeciones a la patentabilidad ya sustentada, el Director de Nuevas Creaciones,

RESUELVE

ARTÍCULO PRIMERO: Denegar la patente de modelo de utilidad para la creación titulada “MECANISMO PARA LA IDENTIFICACIÓN, VALIDACION DE LOS REQUERIMIENTOS DE SEGURIDAD Y ELEMENTOS DE PROTECCIÓN PERSONAL POR PARTE DEL TRABAJADOR PARA REALIZAR LABORES DETERMINADAS EN LA EMPRESA”.

Resolución N° **70158**

Ref. Expediente N° NC2020/0001367

ARTÍCULO SEGUNDO: Notificar el contenido de la presente resolución a CONTROLES INTELIGENTES SAS, advirtiéndole que contra ella procede el recurso de apelación, ante el Superintendente Delegado para la Propiedad Industrial, del cual podrá hacer uso 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 30 de octubre de 2020



Edna Marcela Ramirez Orozco
DIRECTORA DE NUEVAS CREACIONES