



FELIPE FIGUEROA

PROPIEDAD INTELECTUAL - BIOTECNOLOGÍA

Doctor:

JOSÉ LUIS SALAZAR

Director de Nuevas Creaciones

Superintendencia de Industria y Comercio

E. S. D.

SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO



No. 10-161412-00007-0000

Fecha: 2013-01-10 16:31:19 Dep. 2020 DIR NUEVASOR
Tra. 2 PATENTES Eve: 1 REGDEPOSITO
Act. 523 RESPUESTA Folios: 18 **20**

REFERENCIA: Expediente 10-161412 PATENTE DE INVENCION

ASUNTO: Respuesta a requerimiento Art. 45 DA 486/2000.

**“UN METODO PARA VALIDAR Y AUTENTICAR INFORMACION BIOMETRICA DE USUARIOS Y
FUNCIONARIOS EN ENTIDADES REMOTAS”**

1. FELIPE EDUARDO FIGUEROA CARDOZO, identificado como aparece al pie de mi firma, abogado en ejercicio, portador de la Tarjeta Profesional No. 140.243 expedida por el Consejo Superior de la Judicatura, actuando en nombre y representación de TECMED SAS, solicitante de la patente de invención “UN METODO PARA VALIDAR Y AUTENTICAR INFORMACION BIOMETRICA DE USUARIOS Y FUNCIONARIOS EN ENTIDADES REMOTAS”, radicada en el Expediente 10-161412, conforme al poder de representación otorgado que de manera previa se anexó a la actuación administrativa, procedo a dar contestación al auto dictado por ese Despacho, Oficio 15236 del 24 de agosto de 2012 notificado por fijación en lista del 28 de agosto de 2012.

2. Cambio de modalidad de la Solicitud

En atención a los argumentos expuestos por el Señor Examinador frente a los defectos evidenciados en la descripción y en las reivindicaciones de la solicitud, se presenta a su consideración la modificación de la modalidad de la solicitud, en el sentido de transformar la misma a la figura del modelo de utilidad.

felipefigueroac@yahoo.com.mx

Carrera 3 A No. 30-10 Bogotá D.C. (57) (1) 2826279 - 315 2849325

La transformación de la modalidad de protección solicitada a la figura de modelo de utilidad se presenta conforme a lo señalado por el artículo 35 de la Decisión Andina 486 de 2000, teniendo en cuenta que la naturaleza de la solicitud permite proceder en dicho sentido.

En efecto, la transformación de la solicitud a modelo de utilidad se configura en la caracterización del identificador biométrico con la particularidad de que éste dispositivo funciona en un sistema de control y manejo de información que permite identificar el sitio remoto. En otras palabras, el cambio en la modalidad de protección se circunscribe a las características técnicas de los elementos que conforman el dispositivo, cumpliendo con lo normado por el artículo 81 del Régimen Andino de Propiedad Industrial.

En este punto, resulta necesario resaltar que la modificación efectuada se elaboró con base en el sustento descriptivo originalmente presentado y, en consecuencia, no constituye ampliación de la materia divulgada y reivindicada en la solicitud, puesto que, como se dejó sentado en precedencia, el objeto de la modificación versa sobre la explicación detallada de los elementos técnicos que conforman la estructura para validar y autenticar información biométrica de usuarios y funcionarios en entidades remotas a través de elementos de identificación biométrica y redes de seguridad privada que pueden acceder a una pluralidad de bases de datos de identificación biométrica, los cuales, habían sido debidamente mencionados y relacionados en la solicitud inicial, lo cual, permite optar por la modificación de protección propuesta en la presente contestación.

3. De la Solicitud de Patente.

3.1. Del Título de la Solicitud.

Con el propósito de precisar el contenido y alcance del modelo de utilidad propuesto, se presenta un nuevo título que identifica la materia reivindicada, el cual, reemplaza en su totalidad el anteriormente presentado. En estas condiciones, la nueva denominación de la solicitud de protección responde al siguiente título:

felipefigueroac@yahoo.com.mx

Carrera 3 A No. 30-10 Bogotá D.C. (57) (1) 2826279 - 315 2849325

“ESTRUCTURA PARA VALIDAR Y AUTENTICAR INFORMACIÓN BIOMÉTRICA DE USUARIOS Y FUNCIONARIOS EN ENTIDADES REMOTAS”

3.2. De la Memoria Descriptiva y el Capítulo Reivindicatorio.

Con el ánimo de subsanar las objeciones indicadas por el Señor Examinador, se presenta a su consideración un nuevo capítulo descriptivo, compuesto por la explicación detallada de los elementos técnicos que conforman el dispositivo de identificación biométrica.

En este mismo sentido, se presenta para el análisis del Señor Examinador un nuevo pliego reivindicatorio, el cual, reemplaza en su totalidad el originalmente presentado. Este nuevo pliego se encuentra conformado por cinco (5) cláusulas que cumplen a cabalidad con las reglas de claridad y concisión que rigen la presentación del capítulo reivindicatorio y su sustentación guarda total apego a la materia enseñada en la nueva memoria descriptiva que se propone en la presente contestación.

4. Examen de Patentabilidad.

4.1. Nivel Inventivo

El Señor Examinador establece como el estado del arte más cercano a la materia reclamada en la cláusula 1 de la invención originalmente presentada, las patentes norteamericanas US20090216831 “ENTITY IDENTITY MANAGEMENT SYSTEM AND ASSOCIATED METHODS” y US5953441 FINGERPRINT SENSOR HAVING SPOOF REDUCTION FEATURES AND RELATED METHODS, denominados para efectos del presente escrito como Documento D1 y Documento D2, respectivamente.

Luego de realizar el examen de patentabilidad de la solicitud originalmente presentada, concluye el Señor Examinador en el Oficio de Requerimiento, visible a Folio 46, que *“La Reivindicación 1 cumple con el requisito de novedad (Art 16,) pero no cumple con el requisito de nivel inventivo (Art 18)”*.

felipefigueroac@yahoo.com.mx

Carrera 3 A No. 30-10 Bogotá D.C. (57) (1) 2826279 - 315 2849325

3.2. En primer término, resulta preciso señalar que el nuevo pliego reivindicatorio define de forma clara y precisa los elementos técnicos que conforman a la estructura para validar y autenticar información biométrica de usuarios y funcionarios en entidades remotas con la particularidad de que éste dispositivo funciona en un sistema de control y manejo de información que permite identificar el sitio remoto.

Esta particularización de la estructura contenida en el nuevo capítulo reivindicatorio, el cual guarda entero apego a la nueva memoria descriptiva, genera en consecuencia que el modelo de utilidad presentado no se encuentre afectado por el estado del arte relacionado en el Oficio de Requerimiento emitido, esto es, los documentos D1 y D2.

En este sentido, resulta pertinente resaltar que la modificación de la protección a modelo de utilidad no pretende proteger un método, sino una estructura para validar y autenticar información biométrica de usuarios y funcionarios en entidades remotas a través de elementos de identificación biométrica y redes de seguridad privada que pueden acceder a una pluralidad de bases de datos.

En conclusión, el nuevo capítulo reivindicatorio presentado supera las objeciones comentadas por el Señor Examinador, teniendo en cuenta que la modalidad de protección a la que se pretende arribar, es decir, la figura del modelo de utilidad, expone la caracterización de los elementos de manera tal que la configuración de la estructura objeto de solicitud sea susceptible de protección en los términos contemplados por el artículo 81 de la Decisión Andina 486 de 2000, desvirtuando, en consecuencia, la postura expuesta por el Señor Examinador, según la cual la solicitud no constituía una invención en los términos del literal e del artículo 15 de la norma en comento.

De igual forma, el nuevo capítulo reivindicatorio se encuentra por fuera del espectro del alcance de la divulgación contenida en los Documentos D1 y D2, citados por el Señor Examinador como estado del arte cercano, reiterándose que la modificación no constituye ampliación de la materia divulgada y reivindicada en la solicitud original.

4. Anexo

De manera adjunta al presente documento, allego al Expediente:

- Formato Único de Modificación de solicitud en trámite.
- Copia del nuevo capítulo descriptivo en el cual se modifica la solicitud a la protección consagrada por la figura de modelo de utilidad que reemplaza en su totalidad el anteriormente presentado.
- Copia del nuevo capítulo reivindicatorio compuesto por cinco (5) cláusulas que reemplaza en su totalidad el anteriormente presentado.
- Comprobante de consignación de las tasas estatales establecidas para el trámite.

5. PETICIÓN

En virtud de lo anteriormente expuesto, ruego a usted proceder a estudiar nuevamente la Estructura para validar y autenticar información biométrica de usuarios y funcionarios en entidades remotas y, en consecuencia, otorgar el título de modelo de utilidad a la misma.

Del Señor Director de Nuevas Creaciones,



FELIPE EDUARDO FIGUEROA CARDOZO
C.C. 16940582
T.P. 140243 CS de la J.

felipefigueroac@yahoo.com.mx

Carrera 3 A No. 30-10 Bogotá D.C. (57) (1) 2826279 - 315 2849325

DIRECCIÓN DE NUEVAS CREACIONES
CONVERSIÓN, DIVISIÓN Y FUSIÓN DE SOLICITUDES

1. Identificación del Trámite

- ☒ **Conversión** ☐ **División** ☐ **Fusión**
- ☒ Patente de Invención
☐ Patente de Modelo de Utilidad
☐ Registro de Diseño Industrial
☐ Esquema de Trazado de Circuitos Integrados

2. Datos del solicitante

Persona Natural ☐ Persona Jurídica ☒

TECMED SAS

Nombre o denominación / Nombre o razón social
GIOVANNI FAJARDO

Nombre del representante legal
Tipo de empresa Micro ☐ Pequeña ☐ Mediana ☐ Otra ☐

Documento de identificación: ☐ C.C. ☐ C.E. ☒ NIT ☐ Otro Número 900389243-8

Nacionalidad/País de constitución	Dirección del titular	Ciudad
COLOMBIA		
Dirección electrónica	No. Fax	Número telefónico

☐ Autorizo expresamente a la Superintendencia de Industria y Comercio para que todas las comunicaciones sean enviadas a través de la dirección de correo electrónico

3. Datos del apoderado:

FIGUEROA CARDOZO FELIPE EDUARDO **CC 16940582** **140.243 C.S. de la J.**
Apellidos y Nombre Documento de identificación Tarjeta profesional

Dirección y domicilio	Ciudad
Carrera 3 A No. 30-10 Apto 205, Edificio San Diego I	Bogotá D.C.
Dirección electrónica	Número telefónico
felipefigueroac@yahoo.com.mx	315 2849325 – (01) 2826279

En caso de haber presentado poder general para asuntos que se adelanten ante la Delegatura de Propiedad Industrial, sírvase indicar el número de su radicación o protocolo de poder general _____

4. Datos del trámite		
CONVERSION	DIVISION	FUSION
Expediente: 10-161412	Expediente _____	Expediente _____
De: Patente de Invención	_____	_____
A: Patente de Modelo de Utilidad	De: _____	De: _____
	A: _____	A: _____

5. Comprobante de Pago No <u>13-02677</u> Fecha <u>10 / 01 / 2013</u>

6. Anexos
☒ Comprobante de pago de la tasa para la presentación de la corrección y/o modificación
☐ Poder, si fuere el caso con el que se acredita la representación
☐ Número de documento que ordena la comisión o fusión o división
☒ Documento que contiene la conversión, división o fusión de la solicitud
☐ Copia de la solicitud y sus anexos en formato magnético

7. Firma	
FELIPE EDUARDO FIGUEROA CARDOZO	
Nombre y apellidos	Firma
16940582	140243 C.S. de la J.
C.C	Tarjeta Profesional

ESTRUCTURA PARA VALIDAR Y AUTENTICAR INFORMACIÓN BIOMÉTRICA DE USUARIOS Y FUNCIONARIOS EN ENTIDADES REMOTAS

5 CAMPO DE LA INVENCIÓN

La presente invención está relacionada con una estructura para validar y autenticar información biométrica de usuarios y funcionarios en entidades remotas a través de elementos de identificación biométrica y redes de seguridad privada que pueden acceder a una pluralidad de bases de datos.

ANTECEDENTES DE LA INVENCIÓN

En la actualidad la seguridad de la información personal es muy importante en las transacciones y manejo de datos ya que se han establecido nuevos medios de transmisión de información personal de un usuario para determinados propósitos. Por ejemplo, los ciudadanos pueden solicitar diferentes trámites ante determinada autoridad estatal como puede ser la expedición o la renovación de una licencia de conducción; sino se guardan las previsiones del caso, personas malintencionadas podrían valerse de medios tecnológicos para apoderarse fraudulentamente de la identidad de las personas o para hacer aparecer que se han cumplido ciertos requisitos para realizar un trámite, sin que el usuario haya en verdad pasado por un proceso de verificación y validación para la consecución de dicho trámite.

Durante varios años se han realizado numerosos esfuerzos enfocados principalmente a la elaboración de infraestructuras o sistemas que permitan garantizar la validez o la autenticación a los usuarios cuando estos interactúan en el entorno administrativo, comercial o financiero.

En general la seguridad sobre los datos de un usuario determinado podría definirse como los medios para asegurar que la información permanece segura y que el acceso se encuentra controlado. Existen diferentes mecanismos que emplean desarrollos de software o de hardware para encriptar datos y así prevenir que estos sean apropiados fraudulentamente por terceros; sin embargo, existen también programas que pueden ser empleados para acceder a datos protegidos o también para corromper información de tal manera que resulte inaccesible o irrecuperable.

De igual forma se ha venido trabajando en desarrollos de hardware para prevenir el acceso no autorizado a datos e información personal de un determinado usuario a través de dispositivos que permiten el ingreso, la salida y la modificación de diferentes privilegios en un sistema; dichos desarrollos involucran la mayoría de las veces tecnología biométrica, ésta se basa en el reconocimiento de una persona o un usuario por sus rasgos y características físicas; en los sistemas de acceso seguros se emplean para permitir el acceso a sitios físicos o a información almacenada en bases de datos. Se puede decir que las características biométricas de un individuo pueden ser divididas en dos grandes clases: las físicas que están gobernadas por la forma del cuerpo, por ejemplo, las huellas dactilares, el reconocimiento del rostro, la secuencia específica del DNA, la geometría de la mano, el reconocimiento de determinados órganos de la visión y el reconocimiento del humor o el olor de la persona; igualmente se encuentran las características del comportamiento como pueden ser la voz o la forma de caminar.

Un sistema biométrico puede ser empleado para verificar, es decir, se compara una captura biométrica con una plantilla que ha sido guardada previamente para verificar que la persona que intenta acceder es quién dice ser, puede ser empleada conjuntamente con un número de usuario, un número de identificación o una tarjeta inteligente. De igual manera, dicho sistema biométrico puede ser utilizado para identificar, de tal manera que se puede comparar la captura biométrica con una base de datos para identificar a un usuario desconocido.

En desarrollos de sistemas biométricos se tiene por ejemplo la solicitud US2005154920 la cual presenta un método y un aparato para la recolección, distribución y manejo de datos biométricos de un elemento biométrico o de una red de lectores biométricos, dicha red puede ser empleada para mejorar el desempeño de tiempo de atención de usuarios, funciones de control de acceso o cualquier información que sea manejada y almacenada para identificar a una persona en un tiempo determinado y en un dispositivo biométrico remoto determinado. El sistema emplea un servidor biométrico de datos para manejar y mantener plantillas biométricas sobre dispositivos de lectura remotos de acuerdo a una directiva predeterminada, este proceso incrementa la eficiencia y velocidad de los dispositivos biométricos remotos.

También se encuentra la solicitud WO 2008/060725 que presenta un sistema seguro universal de transacciones que comprende un componente de operaciones y recursos, por lo menos un dispositivo de comunicación para permitir la interacción del usuario entre el componente de operaciones y recursos y una ficha de seguridad asociada con cada usuario del sistema. El componente de operaciones y recursos incluye un primer

componente de seguridad biométrico y un segundo componente de seguridad y un componente de comunicación para habilitar la comunicación segura entre el componente de operaciones y recursos y por lo menos una red. Cada dispositivo de comunicación incluye una ficha de interfaz cableada o inalámbrica, un lector biométrico para permitirle al usuario ingresar una lectura biométrica, un componente de comunicación cableado o inalámbrico para permitir la comunicación entre dicho componente de comunicación y el componente de operaciones y recursos, un dispositivo de entrada de información para el usuario y un dispositivo de salida. Cada ficha segura incluye un componente de ficha de seguridad para generar un código de seguridad y un componente de almacenamiento de datos para almacenar datos del usuario. A dicho usuario se le permite el ingreso al componente de operaciones y recursos solamente cuando la ficha segura hace interfaz con la interfaz de ficha del dispositivo de comunicación, la lectura biométrica ingresada por el usuario coincide con una lectura biométrica asociada con la ficha segura en el componente de seguridad biométrica del componente de operaciones y recursos, y el código de seguridad generado por el componente de seguridad de ficha coincide con un código de seguridad correspondiente asociado con la ficha segura en el segundo componente de seguridad del componente de operaciones y recursos.

Sin embargo, estos desarrollos carecen de medios efectivos de seguridad para el manejo de información personal en las transacciones y la gestión de datos cuando estos son tomados en un sitio remoto o entidad administrativa y luego enviados por un sistema de telecomunicaciones hacia una base de datos ya que no existen por ejemplo, mecanismos de contención en los lectores o dispositivos biométricos frente a medidas falsas o erróneas que no correspondan a un determinado usuario, este es el caso de una suplantación de la huella dactilar.

Otro inconveniente de los documentos del estado de la técnica es que no se establecen tiempos mínimos de operación para un determinado proceso adelantado en un entorno administrativo donde un usuario realiza un trámite y éste debe ser procesado por una entidad determinada; dichos procesos de verificación de tiempos mínimos para cada una de las operaciones aumentan la seguridad para los usuarios y también es una herramienta adecuada para medir la eficiencia y la efectividad de la entidad en la cual se lleva determinado trámite o gestión.

DESCRIPCIÓN DETALLADA DE LA INVENCIÓN

El objeto de la presente solicitud es suministrar una estructura para validar y autenticar información biométrica de usuarios y funcionarios en entidades remotas a través de elementos de identificación biométrica y redes de seguridad privada que pueden acceder a una pluralidad de bases de datos.

Otro objeto de la presente solicitud es suministrar dicha estructura para validar y autenticar información biométrica de usuarios de manera que se provean mecanismos de contención en los lectores o dispositivos biométricos frente a medidas falsas o erróneas que no correspondan a un determinado usuario.

Otro objeto de la presente invención es suministrar dicha estructura para validar y autenticar información biométrica de usuarios de manera que se establezcan tiempos mínimos y máximos de operación para un determinado proceso adelantado en un entorno administrativo donde un usuario realiza un trámite y éste debe ser procesado por una entidad determinada con dicha información biométrica.

Describiendo en detalle el objeto de la presente invención se tiene que la estructura para validar y autenticar información biométrica de usuarios y funcionarios en entidades remotas a través de elementos de identificación biométrica y redes de seguridad privada que pueden acceder a una pluralidad de bases de datos, primeramente se compone de un elemento de control y manejo de la información que es un dispositivo computacional central que permite supervisar y controlar variables de proceso a distancia, proporcionando comunicación con los dispositivos de campo (controladores autónomos) y controlando el proceso de forma automática por medio de un elemento de control y manejo de información que registra la información y permite identificar al sitio remoto o entidad administrativa.

Además de ingresar los datos que identifican a dicha entidad, se debe validar la creación o el ingreso de este sitio remoto o entidad administrativa, a través del ingreso de la huella digital de un administrador del sistema en un dispositivo catalogado como un lector que tiene capacidad de detección de un dedo "vivo", la tecnología de detección activa para detectar dedo humano vivo. Este lector es un escáner óptico de huellas dactilares, que emite una señal especial para que el dedo pueda ser autenticado. Esta señal va más allá de la piel humana y después vuelve al sensor en el interior del escáner. La señal de retorno de un dedo humano vivo es única en comparación con la de cualquier otro material. Funciona con un algoritmo para

diferenciar la señal de retorno de dedo vivo humana de la de todos los demás materiales. Como resultado, un escáner óptico de huellas dactilares sólo captura la huella digital de dedos vivos y rechaza todos los demás materiales que pone en él. Dedos falsos hechos de silicona, goma o plastilina por ejemplo no se pueden utilizar para obtener acceso a través de escáner óptico de huellas dactilares. Esto se debe a que el dedo debe tener contacto con un sitio específico en el escáner de huella digital; la resolución de la imagen es de 480 x 320, píxeles 500 DPI, sensor óptico CMOS y cuatro sensores infrarrojos; esto con el fin de evitar que alguien pretenda acceder a la información en dicho sistema de control de manera fraudulenta.

En la estructura para validar y autenticar información biométrica de usuarios y funcionarios en entidades remotas a través de elementos de identificación biométrica y redes de seguridad privada que pueden acceder a una pluralidad de bases de datos, se tiene que a un determinado usuario en dicho sitio remoto o entidad administrativa se le realiza una captura de huella digital para ser ingresado a dicho sistema de control y manejo de la información, a través de un dispositivo catalogado como un lector que tiene capacidad de detección de un dedo "vivo", esto con el fin de evitar que alguien pretenda acceder a un determinado trámite en una entidad o a una base de datos de forma fraudulenta, es decir, con la utilización o el empleo de dedos falsos hechos en silicona o caucho.

Esto se logra a través de la señal que emite el lector biométrico, dicha señal cuando es emitida permite traspasar la piel humana para así comparar el retorno de dicha señal la cual la hace única y distintiva frente a la señal que puedan emitir otros materiales que no correspondan a un dedo "vivo".

En esta estructura también existe una pluralidad de elementos de ingreso de información biométrica adicional del usuario a dicho sistema de control y manejo de la información tal como un elemento de captura fotográfica del rostro de la persona, que es una cámara con sensor digital de alta definición que produce imágenes nítidas con un alto grado de detalle, con sensor nativo HD (Alta Definición), sistema de enfoque automático avanzado, tecnología de lentes que mejoran la calidad de la imagen con nitidez y tecnología de manejo automático de luz para producir imágenes nítidas con alto grado de detalle y contraste, profundidad de color verdadero de 24 bits o superior y función de seguimiento robotizado. La impresión manuscrita de la firma se logra a través de un dispositivo digitalizador de firmas con pantalla LCD monocromática con superficie anti-rayones y lápiz óptico pasivo que muestra el texto de la afirmación de contexto de la firma con mayor nitidez y que es capaz de asignar un número único de

identificación de serie para el equipo, presenta diseño ergonómico y es capaz de producir una vinculación jurídica entre firmas electrónicas; otros elementos de información biométrica adicional donde se realiza la captura digitalizada de la identificación personal de dicho usuario la cual será digitalizada son una pluralidad de lectores bidimensionales con la capacidad de decodificar códigos bidimensionales, capacidad de leer tanto códigos de barras 1D y 2D, con tolerancia al movimiento excepcional, velocidades de lectura rápida al eliminar la necesidad de alinear el código de barras con la línea de exploración, protege contra agua y polvo para un rendimiento fiable, captura de imagen integrada y capacidades de transferencia de interface.

10

El funcionario o empleado del sitio remoto o entidad administrativa valida el ingreso del usuario al sistema de información realizando una captura de su huella digital que ha sido previamente ingresada a dicho sistema de información, a través de un dispositivo catalogado como un lector que tiene capacidad de detección de un dedo "vivo", de manera tal que sin este paso de validación es imposible ingresar la información de dicho usuario a dicho sistema de información.

15

En la estructura para validar y autenticar información biométrica de usuarios y funcionarios en entidades remotas a través de elementos de identificación biométrica y redes de seguridad privada que pueden acceder a una pluralidad de bases de datos, el usuario realiza una interacción en el sitio remoto o entidad administrativa que puede ser por ejemplo un trámite administrativo, médico o financiero en el cual se precisa la identificación biométrica del usuario y la posterior validación del funcionario o empleado del sitio remoto o entidad administrativa. Es de anotar que en este punto la secuencia de identificación del usuario y del empleado o funcionario se realizan tantas veces como trámites sean necesarios, es decir, para una aplicación especial de la estructura de la presente invención como puede ser la obtención de una licencia de conducción o el permiso para el porte de armas, proceso en el cual se ven involucrados una serie de exámenes médicos, psicológicos, de destreza visual y motriz, la interacción del usuario en el sitio remoto o entidad administrativa se repetirá el mismo número de veces que correspondan a los exámenes médicos y de destreza para certificar que dicho usuario es apto para obtener su permiso para portar armas o la consecución de la licencia de conducción.

20

25

30

De manera análoga el funcionario o empleado del sitio remoto o entidad administrativa validará cada uno de los exámenes o trámites que solicite el usuario a través de la estructura de la presente invención de forma que sin este paso de validación por parte de dicho empleado o funcionario no es posible continuar con la solicitud. Es importante

resaltar que la estructura de la presente invención cuenta con mecanismos específicos para establecer tiempo mínimos de operación antes de los cuales no se validaría dicho examen o trámite solicitado por dicho usuario con el fin de evitar un posible fraude en la solicitud del trámite o examen. También es posible establecer tiempos máximos para la respuesta del trámite o examen solicitado con el fin de monitorear la eficiencia de dicho sitio remoto o entidad administrativa, todos estos parametrizados o estandarizados desde el dispositivo o sistema computacional. Este mecanismo específico dentro de la estructura que permite establecer los tiempos mínimos o máximos en los que una transacción estará presente en la estructura se compone de una pluralidad de multi-
10 procesadores de varios núcleos, un módulo controlador lógico programable (PLC), un módulo de memoria Flash, un módulo de memoria RAM, un módulo de Entrada/Salida (AIO), un módulo de comunicaciones GPS con antena, una pluralidad de módulos de comunicaciones múltiples GPRS configurables, una pluralidad de módulos Ethernet TCP/IP, una pluralidad de módulos USB múltiples y un módulo serial.

15 En la estructura para validar y autenticar información biométrica de usuarios y funcionarios en entidades remotas a través de elementos de identificación biométrica y redes de seguridad privada que pueden acceder a una pluralidad de bases de datos, se tiene que la información validada por el funcionario o empleado del sitio remoto o entidad administrativa para un usuario en particular, es certificada por otro funcionario o empleado de dicho sitio remoto o entidad administrativa para conceder o denegar su aprobación del examen o trámite que ha solicitado dicho usuario a través de un dispositivo terminal computacional remota con capacidad de procesamiento, almacenamiento y comunicaciones seguras que se integra a un sistema o dispositivo
20 computacional central que en el caso que se presente un evento o cambio de los estados estandarizados o parametrizados, el controlador en campo debe agregar una espacio de tiempo que marca el momento en que se generó el evento, se marcan los datos producidos con la fecha y la hora en el momento de la lectura. La grabación de estos datos debe permitir una secuencia de eventos, la cual permite almacenar no solo
25 los datos monitoreados sino todos los datos que se producen y en el orden que se produzcan para ser posteriormente analizados en el dispositivo computacional central. El dispositivo computacional remoto genera las alarmas de eventos al dispararse la violación de reglas o parámetros establecidos tales como (equipos o elementos no registrados, manipulación inadecuada de dichos elementos entre otros).

35 En la estructura para validar y autenticar información biométrica de usuarios y funcionarios en entidades remotas a través de elementos de identificación biométrica y redes de seguridad privada que pueden acceder a una pluralidad de bases de datos,

se tiene que dicho sitio remoto o entidad administrativa envía la información referente al perfil del usuario y los resultados del trámite administrativo que ha solicitado dicho usuario en dicho sitio remoto a través de una Red Privada Virtual, donde se establece una conexión segura entre las estaciones clientes del sitio remoto y el administrador de dicho sistema de control y manejo de información central a través de enrutadores multipropósito capaces de realizar la interconexión entre dicho sitio remoto y el administrador de dicho sistema de control; La comunicación a través del dispositivo terminal computacional remoto con capacidad de procesamiento, almacenamiento y comunicaciones seguras que se integra a un sistema o dispositivo computacional central, se logra a través de un elemento de comunicación que se compone de una pluralidad de módulos GPS y un módulo GPRS de comunicación móvil y le permite a dicho dispositivo computacional central comunicarse a través de una Red Privada Virtual a una base de datos de carácter público.

En este punto en la estructura se valida la información enviada por dicho sitio remoto de manera tal que se reconoce si dicha información proviene de la entidad administrativa que previamente ha sido identificada en la estructura; dichos mecanismos de validación están basados en el control de acceso del medio (MAC) y de identificación de etiqueta numérica que corresponde a una interfaz de un dispositivo dentro de una red (IP), identificación de etiqueta alfanumérica de la BIOS, identificación de la memoria RAM y discos duros de las estaciones clientes de dicho sitio remoto.

En la estructura para validar y autenticar información biométrica de usuarios y funcionarios en entidades remotas se tiene que la conexión segura entre las estaciones clientes del sitio remoto y el administrador de dicho sistema de control y manejo de información central puede ser llevada a cabo por medio de una unidad de terminal remota o microprocesador que puede generar la identificación Geofísica de dicho sitio remoto determinada por GPS y además, es capaz de generar una alarma para evitar la posible manipulación o retiro de las estaciones clientes y de los demás dispositivos vinculados en dichos sitio remoto.

En la estructura para validar y autenticar información biométrica de usuarios y funcionarios en entidades remotas a través de elementos de identificación biométrica y redes de seguridad privada que pueden acceder a una pluralidad de bases de datos, se tiene que dicho sistema de control y manejo de información central se comunica a través de una Red Privada Virtual a una base de datos de carácter público, como por ejemplo el Registro Único Nacional de Tránsito para ingresar la información con el fin

de validarla, autorizar la realización de un determinado trámite por un organismo de tránsito y registrar las actualizaciones de la información del trámite aprobado.

- 5 En la estructura para validar y autenticar información biométrica de usuarios y funcionarios en entidades remotas a través de elementos de identificación biométrica y redes de seguridad privada que pueden acceder a una pluralidad de bases de datos, se tiene que una vez que dicho sistema de control y manejo de información central se ha comunicado a través de una Red Privada Virtual con dicha base de datos de carácter público, es capaz de generar un certificado para el usuario el cual es guardado
- 10 y firmado en forma digital, es de anotar que dicho certificado es expedido por dicho sistema de control solamente cuando dicho usuario ha superado con éxito el trámite o los exámenes aplicados con las validaciones y los parámetros anteriormente establecidos por dicho sistema.
- 15 Aunque la presente invención se ha descrito mediante las realizaciones preferentes mostradas no limitativas de la invención, queda entendido que las modificaciones y variaciones que conserven su contenido esencial y elemental se entienden dentro del alcance de las reivindicaciones adjuntas.

REIVINDICACIONES

1. Una estructura para validar y autenticar información biométrica de usuarios y funcionarios en entidades remotas a través de elementos de identificación biométrica y redes de seguridad privada que pueden acceder a una pluralidad de bases de datos caracterizada porque se compone de los siguientes elementos:

a) Un dispositivo computacional central de control y manejo de información con capacidad de procesamiento múltiple, almacenamiento y comunicación segura que registra la información que permite identificar un sitio remoto o entidad administrativa;

b) Un elemento lector de información biométrica que tiene capacidad de detección de un dedo vivo ;

c) Una pluralidad de elementos lectores de información biométrica capaces de tomar información biométrica adicional de un usuario;

d) Un elemento que permite establecer los tiempos mínimos o máximos en los que una transacción estará presente en la estructura de validación y autenticación de información biométrica;

e) Un dispositivo terminal computacional remota con capacidad de procesamiento, almacenamiento y comunicaciones seguras que se integra al dispositivo computacional central.

f) Un elemento de comunicación a través de un dispositivo terminal computacional remoto con capacidad de procesamiento, almacenamiento y comunicaciones seguras que se integra a un sistema o dispositivo computacional central, que le permite a dicho dispositivo computacional central comunicarse a través de una Red Privada Virtual a una base de datos de carácter público;

g) Un elemento de generación de certificados para un usuario el cual es guardado y firmado en forma digital una vez que dicho dispositivo computacional central se ha comunicado a través de una Red Privada Virtual con dicha base de datos de carácter público, a través del

dispositivo terminal computacional remota con capacidad de procesamiento, almacenamiento y comunicaciones seguras.

- 5 2. La estructura para validar y autenticar información biométrica de usuarios y
funcionarios en entidades remotas a través de elementos de identificación
biométrica y redes de seguridad privada que pueden acceder a una pluralidad de
bases de datos de la reivindicación 1 caracterizada porque el elemento lector de
información biométrica que tiene capacidad de detección de un dedo vivo
10 presenta una resolución de imagen de 480 x 320 píxeles, 500 DPI, un sensor
óptico CMOS, y cuatro sensores infrarrojos.
- 15 3. La estructura para validar y autenticar información biométrica de usuarios y
funcionarios en entidades remotas a través de elementos de identificación
biométrica y redes de seguridad privada que pueden acceder a una pluralidad de
bases de datos de la reivindicación 1 caracterizada porque la pluralidad de
elementos lectores de información biométrica se componen de una cámara con
sensor digital de alta definición, un elemento de enfoque automático con
profundidad de color verdadero a 24 bits y función de seguimiento robotizado; un
20 dispositivo digitalizador de firmas con pantalla LCD monocromática con
superficie anti-rayones y lápiz óptico pasivo que produce vinculación entre firmas
electrónicas y, una pluralidad de lectores bidimensionales con la capacidad de
decodificar códigos bidimensionales que pueden leer tanto códigos de barras 1D
y 2D con captura de imagen integrada y capacidades de transferencia de
25 interface.
- 30 4. La estructura para validar y autenticar información biométrica de usuarios y
funcionarios en entidades remotas a través de elementos de identificación
biométrica de la reivindicación 1 caracterizada porque el elemento que permite
establecer los tiempos mínimos o máximos en los que una transacción estará
presente en la estructura se compone de una pluralidad de multi-procesadores
de varios núcleos, un módulo controlador lógico programable (PLC), un módulo
de memoria Flash, un módulo de memoria RAM, un módulo de Entrada/Salida
(AIO), un módulo de comunicaciones GPS con antena, una pluralidad de
35 módulos de comunicaciones múltiples GPRS configurables, una pluralidad de
módulos Ethernet TCP/IP, una pluralidad de módulos USB múltiples y un módulo
serial.

5. La estructura para validar y autenticar información biométrica de usuarios y funcionarios en entidades remotas a través de elementos de identificación biométrica y redes de seguridad privada que pueden acceder a una pluralidad de bases de datos de la reivindicación 1 caracterizada porque el elemento de comunicación que hace parte del dispositivo computacional remoto se compone de una pluralidad de módulos GPS y un módulo GPRS de comunicación móvil.

20

SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO
NIT : 800.176.089-2
- / -

 Industria y Comercio SUPERINTENDENCIA	RECIBO DE CAJA	No. 13 - 002677
		Bogotá D.C., Enero 10 de 2013 - 16:19:26

RECIBIDO DE : TECMED	NI 900.389.243
----------------------	----------------

RE

*** Soporte del Pago ***					
TIPO PAGO	BANCO	CUENTA	No. PAGO	FECHA PAGO	VR. PAGO
CONSIGNACION	BANCO DE BOGOTA	062754387	197804176	10/01/2013	4.000.00
CONSIGNACION	BANCO DE BOGOTA	062754387	505995593	14/11/2012	120.000.00

*** Conceptos Pagados ***			
CANT. RENTISTICO	CONCEPTO	Vr.UNDITARIO	Vr.CONCEPTO
1 50005-01-03 CAMBIO DE MODALIDAD Y MODIFICACIONES EN CREACION CORRECCION A SOLICITUD EN TRAMITE / MODIFICA		124.000.00	124.000.00
			\$124.000.00

SON: **CIENTO VEINTICUATRO MIL PESOS MONEDA CORRIENTE**

Responsable: 

Recibo de Caja Aplicado al Expediente No. _____

SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO



No. 10-161412-00007-0000

Fecha: 2013-01-10 16:31:19 Dep 2020 DIR.NUEVASCR
Tra. 2 PATENTES Eve. 1 REGDEPOSITO
Act. 523 RESPUESTA Folios: 18 20