

REPÚBLICA DE COLOMBIA
SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO

Resolución N° 22713

Ref. Expediente N° NC2017/0003046

Por la cual se otorga una Patente de Invención

EL SUPERINTENDENTE DE INDUSTRIA Y COMERCIO

en ejercicio de sus facultades legales, en especial de las conferidas en el numeral 26 del artículo 3° del Decreto 4886 de 2011, y

CONSIDERANDO:

PRIMERO: Que mediante escrito radicado en esta Superintendencia el 29 de marzo de 2017 con el N° NC2017/0003046, por TELEPERFORMANCE SE, entró a fase nacional la solicitud de patente de invención titulada “MONITOREO ANTI-FRAUDE DE CENTRO DE CONTACTO, DETECCIÓN Y SOLUCIÓN DE PREVENCIÓN”, que corresponde a la solicitud internacional PCT/US2015/048160 del 2 de septiembre de 2015.

SEGUNDO: Que la solicitud fue publicada en la Gaceta de la Propiedad Industrial N° 797 el 30 de junio de 2017, sin que se hubieran presentado oposiciones por parte de terceros.

TERCERO: Que realizado el examen de fondo mediante Oficio N° 12248, notificado el 11 de octubre de 2018, 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.

CUARTO: Que el solicitante mediante escrito radicado bajo el N° NC2017/0003046 el 28 de diciembre de 2018, respondió oportunamente el requerimiento formulado y presentó las reivindicaciones 1 a 15 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.

QUINTO: 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”*.

SEXTO: Que en el presente caso las reivindicaciones 1 a 15 incluidas en el radicado bajo el N° NC2017/0003046 el 28 de diciembre de 2018, cumplen los requisitos indicados en el considerando anterior, toda vez que se refieren a dos métodos de detección de fraude que difieren del estado de la técnica más cercano, US20110010219, en las etapas de determinar información para identificar un agente programado asignado a dicha estación de trabajo en una llamada por primera vez desde una base de datos de empleados; capturar una imagen de un agente posicionado situado en dicha estación de trabajo en relación con una llamada por primera vez, hacer referencia cruzada a dicha imagen de dicho agente



Resolución N° 22713

Ref. Expediente N° NC2017/0003046

posicionado con dicha información y autenticar que dicho agente posicionado es dicho agente programado.

Adicionalmente, estas diferencias no se encuentran sugeridas en el estado de la técnica y, como consecuencia de ello, se evidencia el efecto de detectar una actividad fraudulenta potencial en un centro de llamadas a partir de datos críticos de un usuario, cuando dicho usuario no ha dado autorización; y sumado a lo anterior, la materia reivindicada, es susceptible de aplicación industrial.

En consecuencia, las reivindicaciones 1 a 15 cumplen los requisitos de novedad, nivel inventivo y aplicación industrial establecidos en la normatividad citada en precedencia y este Despacho encuentra procedente conceder para las mismas la patente solicitada.

SEXTO: Que el solicitante en el escrito radicado N° NC2017/0003046 del 29 de marzo de 2017 tituló la invención como: “MONITOREO ANTI-FRAUDE DE CENTRO DE CONTACTO, DETECCIÓN Y SOLUCIÓN DE PREVENCIÓN”. Sin embargo, no se acepta porque dicho título es de carácter general sugiriendo de forma imprecisa la protección, y de acuerdo con el objeto concebido el título de la invención quedará de la siguiente manera **“MÉTODOS DE MONITOREO ANTI-FRAUDE DE CENTRO DE CONTACTO, DETECCIÓN Y SOLUCIÓN DE PREVENCIÓN”**.

Con fundamento en las anteriores consideraciones, el Superintendente de Industria y Comercio,

RESUELVE

ARTÍCULO PRIMERO: Otorgar patente de invención a la solicitud que entró en fase nacional en virtud del Tratado de Cooperación en Materia de Patentes (PCT), para la creación titulada:

“MÉTODOS DE MONITOREO ANTI-FRAUDE DE CENTRO DE CONTACTO, DETECCIÓN Y SOLUCIÓN DE PREVENCIÓN”

Clasificación IPC: H04M 3/51, H04M 3/22.

Reivindicación(es): 1 a 15 incluidas en el radicado bajo el N° NC2017/0003046 el 28 de diciembre de 2018, de acuerdo con el anexo 1.

Titular(es): TELEPERFORMANCE SE.

Domicilio(s): 21/25 rue Balzac. Paris 75008 84121. FRANCIA.

Inventor(es): Evan DAVIS, Mitch FELLING y Lyle HARDY

Prioridad(es) N° 25/06/2015, US (ESTADOS UNIDOS DE AMÉRICA), 14/750,997.
03/09/2014, US (ESTADOS UNIDOS DE AMÉRICA), 62/045,449.

Resolución N° 22713

Ref. Expediente N° NC2017/0003046

Solicitud internacional N°: PCT/US2015/048160

Fecha: 2 de septiembre de 2015.

Vigente desde: 2 de septiembre de 2015

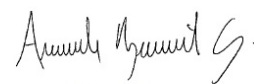
Hasta: 2 de septiembre de 2035

ARTÍCULO SEGUNDO: El titular tendrá los derechos y las obligaciones establecidos en la Decisión 486 de la Comisión de la Comunidad Andina y en las demás disposiciones legales vigentes sobre propiedad industrial, precisando que para mantener vigente la patente se deberá cancelar la tasa anual de mantenimiento, conforme lo dispone el artículo 80 de la referida norma comunitaria.

ARTÍCULO TERCERO: Notificar el contenido de la presente resolución a TELEPERFORMANCE SE, 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 24 de junio de 2019



ANDRÉS BARRETO GONZÁLEZ
SUPERINTENDENTE DE INDUSTRIA Y COMERCIO

Firmado digitalmente
por: ANDRÉS
BERNARDO BARRETO
GONZÁLEZ
Fecha: 2019.06.25
09:01:11 COT
Razón: Validez jurídica.
Ubicación: Bogotá,
Colombia.

ANEXO 1

REIVINDICACIONES CONCEDIDAS

1. Un método (600) de detección de fraude, que comprende: Monitorear actividades (610) de una pluralidad de agentes que asisten a estaciones de trabajo (230) de un centro de contacto (210); Determinar (610) que un agente en una estación de trabajo (230A) de dicho centro de contacto no está en una llamada por primera vez; Determinar (620) que dicho agente está accediendo a un recurso con base en el cliente (240) en dicha primera vez, en el que dicho recurso está asociado con y gestionado por un cliente (270) en un servidor de fondo que está ubicado en una ubicación que es remota de dicho centro de contacto, en el que dicho recurso es accedido por un recurso electrónico en dicha estación de trabajo a través de una red de comunicación (250, 280); y Recolectar (630) evidencia electrónica de dicha estación de trabajo del centro de contacto, en el que dicha evidencia electrónica está asociada con una actividad fraudulenta potencial que se realiza en una primera estación de trabajo, donde dicha actividad fraudulenta potencial comprende acceso no autorizado por dicho agente y se produce cuando: i) se satisface una primera condición cuando dicho agente no está en dicha llamada en dicha primera vez, y ii) se satisface una segunda condición cuando dicho agente está accediendo a dicho recurso en dicha primera vez; en donde dicha recolección de evidencia comprende: Determinar (440) información para identificar un agente programado asignado a dicha estación de trabajo en dicha primera vez desde una base de datos de empleados; Capturar (440) una imagen de un agente posicionado situado en dicha estación de trabajo en relación con dicha primera vez; Hacer referencia cruzada (440) a dicha imagen de dicho agente posicionado con dicha información; Autenticar (440) que dicho agente posicionado es dicho agente programado; y cuando dicho agente posicionado no es dicho agente programado, entonces suministrar notificación que dicha actividad fraudulenta potencia está siendo realizada.
2. El método de la reivindicación 1, en el que dicha determinación de que dicho agente está accediendo a un recurso con base en el cliente comprende además: Determinar (620) que dicho primer agente está accediendo a una aplicación no autorizada de dicho cliente, en donde dicha aplicación no autorizada queda autorizada para acceso cuando dicho agente está activamente en una llamada que proporciona servicios a un cliente de dicho cliente.
3. El método de la reivindicación 1, en el que dicho recurso comprende una base de datos.
4. El método de la reivindicación 1, en el que dicha determinación de que un agente no está en una llamada por primera vez comprende: Determinar (610) que dicho primer agente está disponible para tomar una llamada de un cliente de dicho cliente u otro cliente.
5. El método de la reivindicación 1, en el que dicha evidencia electrónica recogida comprende: Apuntar (630) una cámara (220) colocada para ver dicha estación de trabajo; y Capturar (630) una imagen de dicha estación de trabajo, en la que dicha imagen comprende una vista frontal de dicho agente.



Resolución N° 22713

Ref. Expediente N° NC2017/0003046

6. El método de la reivindicación 1, en el que dicha evidencia electrónica recogida comprende: Activar (630) una cámara (220) colocada en una pantalla de visualización (130) de dicha estación de trabajo; y capturar (630) una imagen de dicha estación de trabajo, en la que dicha imagen comprende una vista frontal de dicho agente.

7. El método de la reivindicación 1, en el que dicha evidencia electrónica recogida comprende: Capturar (630) una imagen de un escritorio de dicha estación de trabajo.

8. El método de la reivindicación 1, que comprende además: Proporcionar (430) una notificación de dicha actividad fraudulenta potencial llevada a cabo en dicha estación de trabajo en un gráfico del centro de contacto (700A), en el que dicho gráfico identifica dichas estaciones de trabajo, en el que un icono (710) representa dicha una estación de trabajo en dicha gráfica, en el que dicho icono está configurado para indicar dicha actividad fraudulenta potencial que se realiza en dicha estación de trabajo.

9. Un método (400, 600) de detección de fraude, en el que dicho método comprende: Monitorear (610) las actividades electrónicas de agentes que asisten a estaciones de trabajo (230) de un centro de contacto (210); Recoger (630) dichas actividades electrónicas que son monitoreadas en una ubicación centralizada; Determinar (410) que se lleva a cabo una actividad fraudulenta potencial en dicho centro de contacto, en donde dicha actividad fraudulenta potencias comprende acceso no autorizado por un agente a dicho recurso a base de cliente; Determinar (420) dicha actividad fraudulenta potencial que se produce en una estación de trabajo (300); Proporcionar (430) una notificación del evento de dicha actividad fraudulenta potencial en un gráfico del centro de contacto (700A), en el que dicho gráfico del centro de contacto indica ubicaciones de cada dichas estaciones de trabajo e información del estado para cada dichas estaciones de trabajo; y Capturar (440) una imagen de dicha estación de trabajo; en el que dicha determinación de que se lleva a cabo una posible actividad fraudulenta en dicho centro de contacto comprende: (610) determinar que un primer agente en dicha estación de trabajo de dicho centro de contacto no está en una llamada por primera vez; (620) determinar que dicho primer agente está accediendo a un recurso basado en el cliente (240) en dicha primera vez, en el que dicho recurso está asociado y gestionado por un cliente (270) en un servidor de fondo que es remoto a dicho centro de contacto, donde se accede a dicho recurso un recurso electrónico en dicha estación de trabajo a través de una red de comunicación (250, 280); y (630) recoger evidencia electrónica de dicha primera estación de trabajo del centro de contacto; en donde dicha recolección de evidencia comprende: Determinar (440) una identidad de un agente posicionado situado en dicha estación de trabajo capturando la primera información para identificar dicho agente posicionado; Determinar (440) una segunda información para identificar un agente programado asignado a dicha estación de trabajo en dicha primera vez accediendo a un registro correspondiente a dicho agente programado de una base de datos de empleados; Hacer referencia cruzada (440) a dicha primera información para identificar dicho agente posicionado con dicha segunda información para identificar dicho agente posicionado; Autenticar (440) que dicho agente posicionado es dicho agente programado cuando dicha primera información para identificar dicho agente posicionado coincide con dicha segunda información para identificar dicho agente programado, en donde dicha notificación de evento comprende una primera información de que dicha actividad fraudulenta potencial está siendo conducida por dicho agente programado; y Determinar (440) que dicho agente



Resolución N° 22713

Ref. Expediente N° NC2017/0003046

posicionado no es dicho agente programado cuando dicha primera información para identificar dicho agente posicionado no coincide con dicha segunda información para identificar dicho agente programado, en donde dicha notificación de eventos comprende una segunda información de que dicha actividad fraudulenta potencial está siendo conducida por un agente no programado para un centro de seguridad (260).

10. El método de la reivindicación 9, en el que dicha captura de una imagen comprende: Apuntar (630) una cámara (220) en dicha estación de trabajo, en el que dicha cámara está posicionada para ver dicha estación de trabajo; Capturar (630) una imagen de una vista frontal de dicha estación de trabajo; y capturar (630) una vista frontal de dicho agente en dicha imagen de dicha vista frontal.

11. El método de la reivindicación 10, que comprende además: Desplazar (440) dicha cámara en una dirección capaz de ver dicha estación de trabajo; Inclinar (440) dicha cámara en un ángulo capaz de ver dicha estación de trabajo; y el zoom (440) de dicha cámara en dicha estación de trabajo.

12. El método de la reivindicación 9, en el que dicha captura de una imagen comprende: Activar (630) una cámara (220) colocada en una pantalla de visualización (130) de dicha estación de trabajo; y Capturar (630) una vista frontal de dicho agente.

13. El método de la reivindicación 9, en el que dicha referencia cruzada a dicha primera información para identificar dicho agente posicionado comprende: Capturar (440) una imagen facial de dicho agente posicionado, en el que dicha primera información para identificar dicho agente posicionado comprende dicha imagen facial; Acceder (440) a una segunda imagen de dicho agente programado en dicho registro; Comparar (440) dicha segunda imagen con dicha imagen facial de dicho agente posicionado; y verificar (440) que dicho agente posicionado sea dicho agente programado cuando dicha segunda imagen coincide con dicha imagen facial.

14. El método de la reivindicación 9, en el que dicha segunda información de determinación para identificar un agente programado además comprende: Capturar (440) la primera información biométrica de un agente que realiza un proceso de inicio de sesión en dicha estación de trabajo; Hacer referencia cruzada (440) a dicha información biométrica con una información biométrica conocida que corresponde con dichos agentes; y Hacer coincidir (440) dicha primera información biométrica capturada con la segunda información biométrica asociada con dicho agente programado.

15. El método de la reivindicación 9, en el que dicha determinación de que se lleva a cabo una actividad fraudulenta potencial comprende además: Determinar (410) una línea de base de transacciones/acciones por dichos agentes, en el que dicha línea de base corresponde a una primera actividad; Identificar (410) una condición atípica que está fuera de dicha línea de base, donde dicha condición atípica corresponde a dicha actividad fraudulenta potencial; y Hacer coincidir (410) la condición atípica con una actividad fraudulenta conocida.