

REIVINDICACIONES

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.

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 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.

P-13176

SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO
DIRECCIÓN DE NUEVAS CREACIONES

E. S. D.

Re: Expediente No. **NC2017/0003046**
Solicitud de patente de Invención a nombre de **TELEPERFORMANCE SE**

Yo, CAROLINA DAZA MONTALVO identificada como aparece al pie de mi firma, domiciliada en la Carrera 11 No. 86-53, obrando como apoderada de la sociedad solicitante **TELEPERFORMANCE SE**, en respuesta al oficio No. **12248** notificado por comunicación electrónica el 11 de octubre de 2018, relacionado con concepto técnico de fondo, me permito manifestar:

1. Modificaciones a la Solicitud

Con fundamento en la facultad que confiere el artículo 34 de la Decisión 486 al solicitante para modificar la solicitud de patente en cualquier momento del trámite, presento junto con este memorial, un nuevo pliego reivindicatorio que comprende 15 reivindicaciones, en donde se realizaron las siguientes modificaciones:

- 1.1 Se modificó la reivindicación independiente 1 con el fin de limitar el alcance de la invención allí definida al incluir las características de las antiguas reivindicaciones dependientes 8 y 9, por lo cual dichas cláusulas han sido eliminadas.
- 1.2 Del mismo modo, se modifica la antigua reivindicación independiente 11 (nueva cláusula 9) con el fin de incluir allí las características de la antigua reivindicación 15.
- 1.3 De otra parte, se elimina la expresión “alejado” de las reivindicaciones independientes 1 y 11.
- 1.4 Finalmente, se renumera todo el pliego reivindicatorio de acuerdo con las modificaciones realizadas y mencionadas anteriormente.

En cuanto a estas modificaciones, es claro que las mismas no amplían de ninguna manera la materia objeto de la presente solicitud y se realizaron con el ánimo de superar las objeciones de claridad y nivel inventivo planteadas por el examinador en su examen de patentabilidad.

2. Pago de tasas

Considerando que el presente memorial se presenta junto con modificaciones a las reivindicaciones, se adjunta recibo por concepto de examen de patentabilidad, según lo establecido en la Resolución 3719 del 2016.

En relación con el número de reivindicaciones, atentamente nos permitimos decir que no se adjunta tasa por reivindicaciones adicionales, toda vez que el nuevo capítulo reivindicatorio contiene un número de cláusulas menor al presentado anteriormente y define en esencia la misma materia objeto.

3. Claridad de las Reivindicaciones

Con relación a la claridad de las reivindicaciones, volvemos sobre el particular que el artículo 30 de la Decisión 486 de la Comunidad Andina establece:

***Artículo 30.-** Las reivindicaciones definirán la materia que se desea proteger mediante la patente. Deben ser claras y concisas y estar enteramente sustentadas por la descripción.*

Respecto a las objeciones de claridad, el solicitante manifiesta que mediante las modificaciones realizadas en el nuevo pliego reivindicatorio quedan subsanadas la totalidad de las objeciones, de modo tal que las nuevas reivindicaciones proporcionan claridad y concisión a la invención descrita, alejando el objeto pretendido de protección de materia no considerada como invención.

Ahora bien, el examinador indica en su concepto técnico que “*La expresión: “línea de base”, de la reivindicación 18; son frases de carácter general que sugieren de forma imprecisa que la protección se extiende a posibles variaciones o modificaciones*”, a lo cual el solicitante muy respetuosamente manifiesta que está en desacuerdo, toda vez que el término objetado es claro y entendible por un experto en la materia, ya que define la base para hacer la determinación a las acciones que deben realizar los agentes del servicio que se desea proteger. Además, este

es un término ampliamente utilizado en el campo de patentes, ya que corresponde a la base (línea base) que se debe tomar en cuenta para realizar una acción.

Por lo tanto, debido a que el término no afecta la forma como se debe interpretar y entender la invención, el mismo se mantiene y no se elimina o reemplaza.

Considerando todos los anteriores argumentos y explicaciones, se considera que se ha respondido a las observaciones hechas por el señor examinador en este respecto, por tanto, se superan las objeciones planteadas y, en consecuencia, las nuevas reivindicaciones 1 a 15 se ajustan a las disposiciones de la Decisión 486/00.

4. Novedad y Nivel inventivo

El examinador establece en su concepto técnico la falta de nivel inventivo por parte de las antiguas reivindicaciones 1 a 18 a la luz de las enseñanzas técnicas descritas en los documentos US 20140208381 (D1) y US 20060023865 (D2).

En este sentido, volvemos sobre el particular que el artículo 18 de la Decisión 486 establece que *“Se considerará que una invención tiene nivel inventivo, si para una persona del oficio normalmente versada en la materia técnica correspondiente, esa invención no hubiese resultado obvia ni se hubiese derivado de manera evidente del estado de la técnica”*.

Se resalta entonces nuevamente que lo anterior significa que el análisis de nivel inventivo NO es una comparación de los objetos de las anterioridades y la solicitud en estudio. El análisis de nivel inventivo debe demostrar la obviedad de la invención y establecer cómo ésta no contiene un salto cualitativo, que demuestre su altura inventiva, teniendo en cuenta que se hace necesario demostrar que la invención analizada carece de nivel inventivo y hubiese sido obvia para una persona versada en la materia.

Considerando la anterior definición, es deseo del solicitante señalar que la combinación de las enseñanzas de D1 y D2 no hace obvia la presente invención definida en las nuevas reivindicaciones 1 a 15 de acuerdo con las razones expuestas a continuación.

Así, considerando las anteriores definiciones y teniendo en cuenta las modificaciones realizadas al capítulo reivindicatorio, es deseo de los Solicitantes presentar argumentos que demuestran el nivel inventivo de la presente solicitud.

En primer lugar, con respecto a la nueva reivindicación independiente 1, la misma define “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 (230.A) 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”, en donde la nueva cláusula independiente incluye ciertas limitaciones que no se encuentran definidas en ningún documento del estado del arte, al tiempo que no hubieran sido obvias para el experto en la materia partiendo de sus conocimientos medios.

A este respecto, es importante mencionar nuevamente que la presente invención es inventiva con respecto a los documentos D1 y D2, toda vez que el documento D1 es silencioso con relación a las limitaciones incluidas en dicha nueva cláusula independiente.

Además, los párrafos 29 a 35 de D2 describen técnicas para identificar un agente y/o determinar la presencia o ausencia de un agente. Sin embargo, la determinación de la identidad de un agente y/o la determinación de si el agente está presente o ausente es diferente de, y no enseña ni sugiere, “*determinar la información para identificar un agente programación asignado a dicha estación de trabajo en dicha primera vez a partir de una base de datos de empleado;... autenticar 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 potencial está siendo realizada*” como se define en las nuevas reivindicaciones independiente 1 y 9 (antigua cláusula 11).

En otras palabras, en la medida que D2 define cuál agente está en una estación de trabajo, dicha anterioridad (tomada sola o en combinación con D1) no enseña ni sugiere la determinación de si el agente es autorizado para estar en esa estación de trabajo (y, de forma inversa, la determinación que el agente no está autorizado para estar en la estación de trabajo). De hecho, el documento D2 en sus párrafos 34 y 35, divulga que un agente se puede sentar y trabajar en cualquier estación de trabajo dada. Esto es, D2 facilita la posibilidad de acceso no autorizado a un recurso basado en cliente en una estación de trabajo, mientras que la invención reivindicada disuade o previene los accesos no autorizados y suministra una notificación que se está realizando un acceso no autorizado (actividad fraudulenta potencial), lo que indica que la presente invención suministra una solución a un problema existente y suple una necesidad que estaba pendiente por ser superada en el estado del arte, mientras que D2 no permite superar el problema, y se mantienen los inconvenientes de seguridad relacionados con los accesos a las estaciones de trabajo por parte de agentes no autorizados y el manejo de información de los clientes a partir de las bases de datos de clientes.

Por lo tanto, el solicitante manifiesta que el efecto técnico y las ventajas asociadas con la invención reivindicada incluyen: detectar cuando se está realizando una actividad fraudulenta potencial (mientras está siendo realizada); tomar las medidas en respuesta a la detección de la actividad fraudulenta potencia, permitiendo así que se puedan tomar otras medidas para remediar esa actividad; y suministrar una acción disuasiva que disuade la actividad fraudulenta potencia.

También es importante tener en cuenta que, al recolectar la evidencia, tal como se indica en las reivindicaciones independientes 1 y 9, se hace mucho más fácil demostrar o probar que se presenta un fraude si esto es necesario, lo cual se presenta claramente en los párrafos 27 y 46 de la descripción como fue presentada originalmente.

Así las cosas, si un experto en la materia tomara las enseñanzas de los documentos D1 y D2 y las combinara, obtendría un método, en efecto, muy similar al definido en la presente invención, pero donde dicho método no permitiría superar los inconvenientes encontrados en el estado del arte, ya que dicho método obtenido no suministraría las herramientas necesarias para evitar las actividades fraudulentas potenciales, ya que no se identificaría el agente en una estación de trabajo dada, ni permitiría la recolección de evidencia para así determinar que se cometió un acto fraudulento, poniendo en riesgo la seguridad de los clientes al divulgar la información personal que se encuentra en las bases de datos, por lo cual la presente invención es inventiva en vista de dichas anterioridades.

De acuerdo con lo definido en los párrafos anteriores, queda claro que la combinación de los documentos D1 y D2 no llevaría a obtener la presente invención como se encuentra definida en las nuevas reivindicaciones 1 a 15, ya que dichas divulgaciones son insuficientes y la única forma de llegar a la presente invención es por medio de un análisis de tipo retrospectivo o “hindsight”, el cual es totalmente inaceptable y no se puede aplicar.

De esta forma, se demuestra que las nuevas reivindicaciones 1 a 15 cumplen con los requisitos de novedad y nivel inventivo, ajustándose de este modo a las definiciones de los artículos 16 y 18 de la Decisión 486/00.

5. Conclusiones

Considerando los argumentos indicados anteriormente, es claro que la invención descrita en las nuevas reivindicaciones 1 a 15 cumple con los requisitos de novedad y nivel inventivo, tal como se define en los artículos 16 y 18 de la Decisión 486/00 y como se explica detalladamente en el Manual Andino y la Guía para Examinadores de la Superintendencia de Industria y Comercio. Así, respetuosamente se solicita que se reconozca la novedad, el nivel inventivo y la aplicación industrial, y, por lo tanto, la

Superintendencia de Industria y Comercio conceda el privilegio de patente para la invención titulada “*MONITOREO ANTI-FRAUDE DEL CENTRO DE CONTACTO Y MÉTODO DE DETECCIÓN DE FRAUDE*” a nombre de TELEPERFORMANCE SE.

Habiendo atendido cabalmente las objeciones presentadas por ese despacho, atentamente solicitamos se conceda el privilegio de patente de invención a la solicitud en estudio o si el señor examinador considera que subsisten razones para objetar la presente invención, rogamos expedir otro examen de fondo con los debidos motivos y razones que sustenten su objeción con el fin de que nuestro mandante tenga la posibilidad de exponer sus argumentos con base en la interpretación de los artículos 45 de la Decisión 486 -el cual otorga la facultad al examinador para emitir los exámenes de fondo- y 42 del Código de Procedimiento Administrativo y de lo Contencioso Administrativo que señala que: “*Habiéndose dado oportunidad a los interesados para expresar sus opiniones, y con base en las pruebas e informes disponibles, se tomará la decisión, que será motivada. La decisión resolverá todas las peticiones que hayan sido oportunamente planteadas dentro de la actuación por el peticionario y por los terceros reconocidos*”, (el subrayado es nuestro).

En consecuencia, solicitamos a ese despacho pronunciarse en relación con todos los argumentos presentados en este memorial dando estricta aplicación al principio del debido proceso consagrado en el artículo 29 de la Constitución Nacional.

6. Anexos

- Nuevo capítulo reivindicatorio compuesto por 15 reivindicaciones.
- Comprobante de pago por concepto de examen de patentabilidad.

Señor Director,


CAROLINA DAZA MONTALVO
C.C. 66.783.790 de Palmira Valle
TP-141563 CSJ
notificaciones@clarkemodet.com.co

www.clarkemodet.com

ESPAÑA · PORTUGAL · ARGENTINA · BRASIL · CHILE · COLOMBIA · MÉXICO · PERÚ · URUGUAY · VENEZUELA

REIVINDICACIONES

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;

www.clarkemodet.com

ESPAÑA · PORTUGAL · ARGENTINA · BRASIL · CHILE · COLOMBIA · MÉXICO · PERÚ · URUGUAY · VENEZUELA

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.

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 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.



SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO

NIT: 800.176.089-2

COMPROBANTE DE RECAUDO SISTEMA SIPI

Radicado: NC2017/0003046
Recibo: 18-99708
Fecha: 28/12/2018

CAROLINA MERCEDES DAZA MONTALVO
CC: 66.783.790
Pago PSE No: 247431
CUS: 399537378

Patente PCT
MONITOREO ANTI-FRAUDE DE CENTRO DE CONTACTO, DETECCIÓN Y SOLUCIÓN DE PREVENCIÓN

Detalle del pago

Id.	Rentístico	Concepto y Servicio	Cant.	Val. Unit.	Subtotal
1	50005-01-01	Solicitud examen de patentabilidad Patente de Invención (DESCUENTO INTERNET)	1	\$ 1,053,500	\$ 1,053,500
TOTAL					\$ 1,053,500