

Señores

Superintendencia de Industria y Comercio

Dirección de Nuevas Creaciones

E. S. D.

Ref: Expediente No. NC2019/0008341.

Solicitud de registro de Patente de Invención denominada “MÉTODO, SISTEMA Y DISPOSITIVO DE ALMACENAMIENTO DE ANÁLISIS DE SEÑALES MÚLTIPLES PARA LA IDENTIFICACIÓN DE ÁMBITO AFECTADO”.

Fase nacional de la solicitud PCT/US2018/017817.

Solicitante: MICROSOFT TECHNOLOGY LICENSING, LLC.

Luz Helena Adarve, identificada como aparece al pie de mi firma, y obrando en mi condición de apoderada de **MICROSOFT TECHNOLOGY LICENSING, LLC**, solicitante de la patente en referencia, a continuación, doy respuesta al Oficio **No. 11738** del 23 de julio de 2021.

1. Respecto al título de la solicitud

En el numeral 2.1 del oficio No. **11738**, se presentan las siguientes observaciones sobre el título de la solicitud:

“El nombre de la invención de que se trata en el artículo 27 literal d) de la Decisión 486 deberá reflejar el objeto y el campo industrial con el cual se relaciona la misma y ser concordante con la materia descrita y las reivindicaciones de la solicitud. El nombre no podrá referirse a nombres personales, marcas de productos o nombres de fantasía.

El solicitante en el escrito radicado bajo el N° NC2019/0008341 el 30 de julio de 2019, tituló la invención como: ‘ANÁLISIS DE SEÑALES

MÚLTIPLES PARA LA IDENTIFICACIÓN DE ÁMBITO AFECTADO’.
Este título no se relaciona con el objeto de la solicitud contenido en la descripción y las reivindicaciones, por lo cual se sugiere el título siguiente: ‘MÉTODO, SISTEMA Y DISPOSITIVO DE ALMACENAMIENTO DE ANÁLISIS DE SEÑALES MÚLTIPLES PARA LA IDENTIFICACIÓN DE ÁMBITO AFECTADO’.

Con el objetivo de superar esta objeción, es deseo del solicitante cambiar el título de la solicitud al siguiente:

“MÉTODO, SISTEMA Y DISPOSITIVO DE ALMACENAMIENTO DE ANÁLISIS DE SEÑALES MÚLTIPLES PARA LA IDENTIFICACIÓN DE ÁMBITO AFECTADO”

2. Respecto a las Objeciones a la Claridad y Concisión de las reivindicaciones (Artículo. 30 de la Decisión 486).

En el numeral 2.2 del oficio No. **11738**, se presenta la siguiente sugerencia sobre la claridad de las reivindicaciones:

“Se sugiere incluir entre paréntesis () los números de referencia de cada uno de los elementos que hacen parte de la invención de acuerdo con la numeración empleada en los dibujos, con el fin, de hacer más fácil la comprensión de la materia reivindicada”.

Sobre esta sugerencia, se indica que el nuevo capítulo reivindicatorio que se presenta junto con esta respuesta ahora incluye dichos números de referencia.

3. Respecto a la Determinación del Estado de la Técnica y al Examen de Patentabilidad

En los numerales 3, 4 y 5 del oficio citado, ese Despacho concluye que las reivindicaciones de la presente solicitud de patente carecen de novedad y/o nivel inventivo frente a las enseñanzas de los documentos **US2007294187A1** (D1), **US8122122B1** (D2) y **US9516053B1** (D3).

3.1. Novedad y nivel inventivo

Aunque el Examinador haya citado los documentos D1, D2 y D3 para objetar la novedad y la altura inventiva de la presente invención, es posible afirmar que éstos no enseñan las características esenciales de la invención del nuevo capítulo reivindicatorio que ahora se presenta.

Con el fin de superar las objeciones presentadas respecto a la novedad y nivel inventivo de las reivindicaciones, **es deseo del solicitante presentar un nuevo capítulo reivindicatorio compuesto por 20 reivindicaciones**, que encuentran su debido sustento en las reivindicaciones y la descripción originalmente presentadas, sin que ello conlleve ampliación de la invención.

Primero se indica que las anteriores reivindicaciones 1, 9, y 15, correspondiente a las reivindicaciones modificadas 1, 11 y 17, se modificaron con el objetivo de que sea aún más clara su novedad y nivel inventivo ahora incluye las siguientes características que no son divulgadas ni sugeridas por los documentos D1, D2 o D3:

- Las reivindicaciones modificadas 1 y 17 ahora incluyen:
 - *“en donde los resultados de detección son puntuados con base en una proporción entre un recuento de subpoblación y un recuento de población para el comportamiento dentro del servicio en línea (110)”;*
y
 - *“excluir los resultados de detección puntuados que tienen uno o más de un recuento de subpoblación y un recuento de población para el comportamiento por debajo de uno o más de un umbral de subpoblación y un umbral de población, respectivamente”.*
- La reivindicación modificada 11 ahora incluye:
 - *“determinar el grado al cual un comportamiento asociado con el determinado resultado de detección ha sido anteriormente observado que ocurre en el servicio en línea (110) al determinar un recuento de subpoblación y un recuento de población para el comportamiento en el servicio en línea (110)”;*

- “*producir una puntuación de anomalía que será asociada con el resultado de detección dado basándose en una proporción entre un recuento de subpoblación y un recuento de población para el comportamiento*”; y
- “*determinar que el recuento de subpoblación y el recuento de población para el comportamiento está por encima de un umbral de subpoblación y un umbral de población, respectivamente*”.

Estas modificaciones no amplían materia y encuentran su sustento en las páginas 5, 6 y 11 del capítulo descriptivo de la presente solicitud.

Estas características mejoran la resolución del problema técnico de detección de ámbitos comprometidos al puntuar específicamente los resultados de detección, mejorando así la seguridad de los datos alojados en un ordenador (véanse, por ejemplo, los párrafos [0003] y [0004] del documento D1). Por tanto, los rasgos característicos de las nuevas reivindicaciones independientes contribuyen a la presencia de una actividad inventiva.

El documento D1 da a conocer la detección de anomalías en una pluralidad de observaciones de red en tiempo real recopiladas de un flujo de tráfico de red (Ver Resumen del documento D1). En los párrafos [0085] y [0086], el documento D1 describe la asignación de una puntuación sorpresa que indica anomalías a cada observación en función de un modelo, donde el modelo asigna la puntuación en función de la proporción del número de observaciones que coinciden con cada variable asociada con un conjunto de observaciones sobre el número total de observaciones. Sin embargo, el documento D1 no enseña ni sugiere la comparación con valores umbral para la exclusión de resultados del modelo particularmente en función de los umbrales de subpoblación y población (por ejemplo, para evitar que las observaciones con números bajos interfieran con la confiabilidad de los resultados)".

Por su parte los documentos D2 y D3, no sugieren ni divulgan estas características distintivas, y, por lo tanto, no subsanan las falencias del documento D1 en divulgar la invención de la presente solicitud. Esto hace que la presente solicitud no solo sea novedosa, sino también inventiva.

Por lo anterior se concluye que las reivindicaciones independientes en cuestión poseen características que no se dan a conocer de manera obvia para una

persona versada en la materia por los documentos D1, D2 o D3, por ende, la presente invención debe ser considerada como novedosa y con nivel inventivo sobre el estado de la técnica presentado por el Examinador.

4. Conclusión

Los argumentos expuestos en el numeral 3 del presente escrito ponen de manifiesto de una manera clara y contundente que lo revelado en las nuevas reivindicaciones de la presente solicitud resulta completamente NOVEDOSO E INVENTIVO sobre las enseñanzas del estado del arte más cercano representado por los documentos D1, D2 y D3, toda vez que nada dentro de dichos documentos revela en forma directa o al menos llega a sugerir las características distintivas de la invención como lo hace ahora la solicitud. Por consiguiente, no se puede derivar la inexistencia de los requisitos de ley para la concesión del privilegio de patentabilidad.

En consecuencia, me permito solicitar a ese Despacho, proceder con la revisión de las modificaciones y de los argumentos aquí presentados, para conceder el privilegio de patente solicitado para la materia objeto de las 20 reivindicaciones ahora presentadas en el capítulo reivindicatorio modificado, y que de subsistir alguna duda o inquietud respecto a la patentabilidad de la presente invención, a pesar de las modificaciones y argumentos técnicos ahora presentados, sin apartarse del espíritu inventivo originalmente revelado en la solicitud internacional, se le brinde la oportunidad al solicitante de aclararla o de limitar aún más la invención, mediante la emisión de un segundo examen de fondo, teniendo en cuenta el nuevo capítulo reivindicatorio que se somete a revisión, antes de que se emita una decisión definitiva por parte de ese Despacho, de conformidad con lo dispuesto en 1.2.2.5.1 del artículo primero de la Resolución 54093 de 2012.

5. Anexos

Junto con este escrito se incluye lo siguiente:

- Capítulo reivindicatorio modificado, en donde se han llevado a cabo las modificaciones mencionadas anteriormente.

6. Pagos

Junto con esta respuesta se paga la tasa correspondiente a la modificación del capítulo reivindicatorio y a 5 reivindicaciones adicionales.

Petición

Solicito al Despacho, y en el evento que el examinador considere que pese a las modificaciones presentadas aún existen objeciones, que proceda a emitir un segundo examen de fondo sobre el nuevo capítulo reivindicatorio presentado.

En este sentido requiero se me comunique a través del SIPI o cualquier otro medio la existencia de estas objeciones para, de esta manera, si procede, realizar el nuevo pago del examen de patentabilidad de la solicitud de la referencia.

Atentamente,



LUZ HELENA ADARVE GÓMEZ.

C.C 41.575.435 de Bogotá.

T.P. 14.884 C.S.J.

FJG

P-1083

REIVINDICACIONES (con marcas de modificación)

1. Un método (500) para detectar ámbitos comprometidos en un servicio en línea (110), que comprende:
 - recibir (510) resultados de detección de comportamientos que ocurren en los dispositivos dentro del servicio en línea (110);
 - ~~la puntuación de~~ puntuar (520) los resultados de detección basándose en cómo los comportamientos anómalos asociados están dentro del servicio en línea (110), en donde los resultados de detección son puntuados con base en una proporción entre un recuento de subpoblación y un recuento de población para el comportamiento dentro del servicio en línea (110);
 - excluir los resultados de detección puntuados que tienen uno o más de un recuento de subpoblación y un recuento de población para el comportamiento por debajo de uno o más de un umbral de subpoblación y un umbral de población, respectivamente;
 - organizar (530) los resultados de detección puntuados restantes de acuerdo con los ámbitos;
 - aplicar (540) la lógica de detección de señales múltiples a un ámbito determinado para producir una puntuación de confianza que indica si el ámbito determinado está comprometido;
 - determinar (550) si desea presentar una alerta de si el ámbito determinado está comprometido con base en la comparación de la puntuación de confianza con un umbral de alerta; y
 - en respuesta a la determinación de que la alerta se va a presentar del ámbito determinado que está comprometido, generar y transmitir la alerta (560).
2. El método (500) de acuerdo con la reivindicación 1, en donde el ámbito determinado está asociado con un dispositivo determinado o una cuenta de usuario dada en el servicio en línea (110).
3. El método (500) de acuerdo con la reivindicación 1, en donde la puntuación (520) de los resultados de detección además comprende:
 - calcular (600) un identificador para un determinado resultado de detección;
 - recuperar (620) una cuenta de agregado para el resultado de detección dado;
 - incrementar (630) los recuentos de población agregados para el resultado de detección dado;
 - calcular (640) una puntuación de anomalía para el resultado de detección dado basándose en los recuentos de población agregados; y
 - asociar la puntuación de anomalía con el resultado de detección dado para producir un resultado de detección ~~calificado~~ puntuado.
4. El método (500) de acuerdo con la reivindicación 3, en donde los recuentos de población de agregado incluyen:
 - un recuento de población sin procesar, que se incrementa para cada resultado de detección observado; y

al menos un recuento de subpoblación, que se incrementa para cada resultado de detección observado que incluye una característica que define una subpoblación de resultados de detección.

5. El método (500) de acuerdo con la reivindicación 3, en donde el identificador incluye al menos un campo del resultado de detección dado, que incluye:

un papel para un dispositivo dado asociado con el resultado de detección dado;
un usuario asociado con el resultado de detección dado;
una clase de comportamiento asociado con el resultado de detección dado; y
una marca de tiempo.

6. El método (500) de acuerdo con la reivindicación 1, en donde la organización (530) de los resultados de detección puntuados de acuerdo con los ámbitos además comprende:

recibir una definición de ámbito identificando una característica a través de la cual se dividen los resultados de detección;

recibir una ventana de tiempo ~~desde la hora actual~~ a través de la cual los resultados de detección se van a analizar ~~y se observaron~~; y

dividir los resultados de detección que se observaron dentro de la ventana de tiempo en los ámbitos de acuerdo con los valores de la característica identificada incluidos en los resultados de detección.

7. El método (500) de acuerdo con la reivindicación 6, en donde la característica especifica valores para:

Identificadores de dispositivos;
cuentas de usuario; e
Identificadores de procesos.

~~68.~~ El método (500) de acuerdo con la reivindicación 1, en donde los resultados de detección desde una ventana de tiempo más pequeña, que comprende varios minutos de resultados de detección y una ventana de tiempo más grande, que comprende varios días de resultados de detección, se incluyen en los ámbitos.

~~79.~~ El método (500) de acuerdo con la reivindicación 1, en donde la aplicación (540) de lógica de detección de señales múltiples al ámbito determinado para producir la puntuación de confianza además comprende:

seleccionar (710) un modelo predictivo;
extraer (720) características de los resultados de detección;
~~la puntuación puntuar (730) de~~ las características para la conversión en características valoradas numéricamente; y

proporcionar [\(740\)](#) las características del modelo predictivo para generar la puntuación de confianza.

[810.](#) El método [\(500\)](#) de acuerdo con la reivindicación [79](#), en donde el modelo predictivo se genera y selecciona en función de un proceso de aprendizaje continuo de máquina.

[911.](#) Un sistema que incluye un procesador [\(802; 906\)](#) y un dispositivo de almacenamiento de memoria [\(804; 962\)](#) que almacena instrucciones que cuando se ejecutan por el procesador ofrecen detectar ámbitos comprometidos en un servicio en línea [\(110\)](#), que comprende:

un calificador de anomalía de firma, configurado para:

recibir un determinado resultado de detección de un evento observado que ocurre en el servicio en línea [\(110\)](#);

determinar el grado al cual un comportamiento asociado con el determinado resultado de detección ha sido anteriormente observado que ocurre en el servicio en línea [\(110\)](#) al determinar un recuento de subpoblación y un recuento de población para el comportamiento en el servicio en línea [\(110\)](#); y

producir una puntuación de anomalía que será asociada con el resultado de detección dado basándose en una proporción entre un recuento de subpoblación y un recuento de población para el comportamiento-el grado al cual el comportamiento ha sido anteriormente observado; y

determinar que el recuento de subpoblación y el recuento de población para el comportamiento está por encima de un umbral de subpoblación y un umbral de población, respectivamente; y

un detector de señales múltiples en comunicación con el calificador de anomalía de firma, configurado para:

recibir uno o más resultados de detección que comparten un ámbito en el servicio en línea [\(110\)](#) con el resultado de detección dado;

recibir, del calificador de anomalía de firma, la puntuación de anomalía asociada con el resultado de detección;

extraer las características de l resultado de detección dado y de los uno o más resultados de detección que comparten el ámbito, las características incluyendo la puntuación de anomalía; y

generar una puntuación de confianza basándose en las características extraídas de si el ámbito está comprometido.

[1012.](#) El sistema de acuerdo con la reivindicación [911](#), en donde el uno o más resultados de detección compartiendo el ámbito en el servicio en línea [\(110\)](#) con el resultado de detección dado son observados dentro de una ventana de tiempo.

~~1413.~~ El sistema de acuerdo con la reivindicación ~~1012~~, en donde el grado al cual el comportamiento asociado con el resultado de detección dado ha sido observado anteriormente que ocurre en el servicio en línea (110) se basa en ocurrencias durante la ventana de tiempo.

~~1414.~~ El sistema de acuerdo con la reivindicación 911, en donde el grado al cual el comportamiento asociado con el resultado de detección dado ha sido anteriormente observado que ocurre en el servicio en línea (110) se basa en:

un recuento de población sin procesar de los eventos que ocurren en el servicio en línea (110);
y

un recuento de subpoblación sin procesar de un número de ocurrencias del comportamiento en el servicio en línea (110).

~~1315.~~ El sistema de acuerdo con la reivindicación 911, en donde el grado al cual el comportamiento asociado con el resultado de detección dado ha sido anteriormente observado que ocurre en el servicio en línea (110) se basa en:

un recuento de población de ámbito de un número de entidades que comprenden el ámbito del servicio en línea (110); y

un recuento de subpoblación de ámbito de un número de entidades en el ámbito asociado con el comportamiento.

~~1416.~~ El sistema de acuerdo con la reivindicación ~~1315~~, en donde las entidades que comprenden el ámbito se definen por un analista como uno de los dispositivos dentro del servicio en línea (110) o cuentas de usuario del servicio en línea (110).

~~1517.~~ Un dispositivo de almacenamiento legible por computadora que incluye instrucciones ejecutables por procesador para detectar ámbitos comprometidos en un servicio en línea (110), que comprende:

recibir (510) resultados de detección de comportamientos que ocurren en los dispositivos dentro del servicio en línea (110);

~~la puntuación-puntuar (520)~~ de los resultados de detección basándose en cómo los comportamientos anómalos ~~asociados~~ están dentro del servicio en línea (110), en donde los resultados de detección son puntuados con base en una proporción entre un recuento de subpoblación y un recuento de población para el comportamiento dentro del servicio en línea (110);
excluir los resultados de detección puntuados que tienen uno o más de un recuento de subpoblación y un recuento de población para el comportamiento por debajo de uno o más de un umbral de subpoblación y un umbral de población, respectivamente;

organizar (530) los resultados de detección ~~calificados-puntuados restantes según de acuerdo con~~ los ámbitos, en donde un ámbito dado está asociado con un dispositivo dado o una determinada cuenta de usuario en el servicio en línea (110);

aplicar (540) la lógica de detección de señales múltiples al ámbito determinado para producir una puntuación de confianza que indica si el ámbito determinado está comprometido;

determinar (550) si alertar a un analista del ámbito determinado que está comprometido en función de comparar la puntuación de confianza con un umbral de alerta; y

en respuesta a la determinación de que el analista va a ser alertado del ámbito determinado que está comprometido, generar y transmitir una alerta (560).

18. El dispositivo de almacenamiento legible por computadora de acuerdo con la reivindicación 17, en donde la puntuación (520) de los resultados de detección además comprende:

calcular (600) un identificador para un determinado resultado de detección;

recuperar (620) una cuenta de agregado para el resultado de detección dado;

incrementar (630) los recuentos de población agregados para el resultado de detección dado;

calcular (640) una puntuación de anomalía para el resultado de detección dado basándose en los recuentos de población agregados; y

asociar la puntuación de anomalía con el resultado de detección dado para producir un resultado de detección puntuado.

19. El dispositivo de almacenamiento legible por computadora de acuerdo con la reivindicación 17, en donde la organización (530) de los resultados de detección puntuados de acuerdo con los ámbitos además comprende:

recibir una definición de ámbito identificando una característica a través de la cual se dividen los resultados de detección;

recibir una ventana de tiempo a través de la cual los resultados de detección se van a analizar;

y

dividir los resultados de detección que se observaron dentro de la ventana de tiempo en los ámbitos de acuerdo con los valores de la característica identificada incluidos en los resultados de detección.

20. El dispositivo de almacenamiento legible por computadora de acuerdo con la reivindicación 17, en donde la aplicación (540) de lógica de detección de señales múltiples al ámbito determinado para producir la puntuación de confianza además comprende:

seleccionar (710) un modelo predictivo;

extraer (720) características de los resultados de detección;

puntuar (730) las características para la conversión en características valoradas numéricamente; y

proporcionar (740) las características del modelo predictivo para generar la puntuación de confianza.

REIVINDICACIONES

1. Un método (500) para detectar ámbitos comprometidos en un servicio en línea (110), que comprende:

recibir (510) resultados de detección de comportamientos que ocurren en los dispositivos dentro del servicio en línea (110);

puntuar (520) los resultados de detección basándose en cómo los comportamientos anómalos asociados están dentro del servicio en línea (110), en donde los resultados de detección son puntuados con base en una proporción entre un recuento de subpoblación y un recuento de población para el comportamiento dentro del servicio en línea (110);

excluir los resultados de detección puntuados que tienen uno o más de un recuento de subpoblación y un recuento de población para el comportamiento por debajo de uno o más de un umbral de subpoblación y un umbral de población, respectivamente;

organizar (530) los resultados de detección puntuados restantes de acuerdo con los ámbitos;

aplicar (540) la lógica de detección de señales múltiples a un ámbito determinado para producir una puntuación de confianza que indica si el ámbito determinado está comprometido;

determinar (550) si desea presentar una alerta de si el ámbito determinado está comprometido con base en la comparación de la puntuación de confianza con un umbral de alerta; y

en respuesta a la determinación de que la alerta se va a presentar del ámbito determinado que está comprometido, generar y transmitir la alerta (560).

2. El método (500) de acuerdo con la reivindicación 1, en donde el ámbito determinado está asociado con un dispositivo determinado o una cuenta de usuario dada en el servicio en línea (110).

3. El método (500) de acuerdo con la reivindicación 1, en donde la puntuación (520) de los resultados de detección además comprende:

calcular (600) un identificador para un determinado resultado de detección;

recuperar (620) una cuenta de agregado para el resultado de detección dado;

incrementar (630) los recuentos de población agregados para el resultado de detección dado;

calcular (640) una puntuación de anomalía para el resultado de detección dado basándose en los recuentos de población agregados; y

asociar la puntuación de anomalía con el resultado de detección dado para producir un resultado de detección puntuado.

4. El método (500) de acuerdo con la reivindicación 3, en donde los recuentos de población de agregado incluyen:

un recuento de población sin procesar, que se incrementa para cada resultado de detección observado; y

al menos un recuento de subpoblación, que se incrementa para cada resultado de detección observado que incluye una característica que define una subpoblación de resultados de detección.

5. El método (500) de acuerdo con la reivindicación 3, en donde el identificador incluye al menos un campo del resultado de detección dado, que incluye:

- un papel para un dispositivo dado asociado con el resultado de detección dado;
- un usuario asociado con el resultado de detección dado;
- una clase de comportamiento asociado con el resultado de detección dado; y
- una marca de tiempo.

6. El método (500) de acuerdo con la reivindicación 1, en donde la organización (530) de los resultados de detección puntuados de acuerdo con los ámbitos además comprende:

recibir una definición de ámbito identificando una característica a través de la cual se dividen los resultados de detección;

recibir una ventana de tiempo a través de la cual los resultados de detección se van a analizar;
y

dividir los resultados de detección que se observaron dentro de la ventana de tiempo en los ámbitos de acuerdo con los valores de la característica identificada incluidos en los resultados de detección.

7. El método (500) de acuerdo con la reivindicación 6, en donde la característica especifica valores para:

- Identificadores de dispositivos;
- cuentas de usuario; e
- Identificadores de procesos.

8. El método (500) de acuerdo con la reivindicación 1, en donde los resultados de detección desde una ventana de tiempo más pequeña, que comprende varios minutos de resultados de detección y una ventana de tiempo más grande, que comprende varios días de resultados de detección, se incluyen en los ámbitos.

9. El método (500) de acuerdo con la reivindicación 1, en donde la aplicación (540) de lógica de detección de señales múltiples al ámbito determinado para producir la puntuación de confianza además comprende:

- seleccionar (710) un modelo predictivo;
- extraer (720) características de los resultados de detección;
- puntuar (730) las características para la conversión en características valoradas numéricamente; y

proporcionar (740) las características del modelo predictivo para generar la puntuación de confianza.

10. El método (500) de acuerdo con la reivindicación 9, en donde el modelo predictivo se genera y selecciona en función de un proceso de aprendizaje continuo de máquina.

11. Un sistema que incluye un procesador (802; 906) y un dispositivo de almacenamiento de memoria (804; 962) que almacena instrucciones que cuando se ejecutan por el procesador ofrecen detectar ámbitos comprometidos en un servicio en línea (110), que comprende:

un calificador de anomalía de firma, configurado para:

recibir un determinado resultado de detección de un evento observado que ocurre en el servicio en línea (110);

determinar el grado al cual un comportamiento asociado con el determinado resultado de detección ha sido anteriormente observado que ocurre en el servicio en línea (110) al determinar un recuento de subpoblación y un recuento de población para el comportamiento en el servicio en línea (110);

producir una puntuación de anomalía que será asociada con el resultado de detección dado basándose en una proporción entre un recuento de subpoblación y un recuento de población para el comportamiento; y

determinar que el recuento de subpoblación y el recuento de población para el comportamiento está por encima de un umbral de subpoblación y un umbral de población, respectivamente; y

un detector de señales múltiples en comunicación con el calificador de anomalía de firma, configurado para:

recibir uno o más resultados de detección que comparten un ámbito en el servicio en línea (110) con el resultado de detección dado;

recibir, del calificador de anomalía de firma, la puntuación de anomalía asociada con el resultado de detección;

extraer las características del resultado de detección dado y de uno o más resultados de detección que comparten el ámbito, las características incluyendo la puntuación de anomalía; y

generar una puntuación de confianza basándose en las características extraídas de si el ámbito está comprometido.

12. El sistema de acuerdo con la reivindicación 11, en donde el uno o más resultados de detección compartiendo el ámbito en el servicio en línea (110) con el resultado de detección dado son observados dentro de una ventana de tiempo.

13. El sistema de acuerdo con la reivindicación 12, en donde el grado al cual el comportamiento asociado con el resultado de detección dado ha sido observado anteriormente que ocurre en el servicio en línea (110) se basa en ocurrencias durante la ventana de tiempo.

14. El sistema de acuerdo con la reivindicación 11, en donde el grado al cual el comportamiento asociado con el resultado de detección dado ha sido anteriormente observado que ocurre en el servicio en línea (110) se basa en:

un recuento de población sin procesar de los eventos que ocurren en el servicio en línea (110);
y

un recuento de subpoblación sin procesar de un número de ocurrencias del comportamiento en el servicio en línea (110).

15. El sistema de acuerdo con la reivindicación 11, en donde el grado al cual el comportamiento asociado con el resultado de detección dado ha sido anteriormente observado que ocurre en el servicio en línea (110) se basa en:

un recuento de población de ámbito de un número de entidades que comprenden el ámbito del servicio en línea (110); y

un recuento de subpoblación de ámbito de un número de entidades en el ámbito asociado con el comportamiento.

16. El sistema de acuerdo con la reivindicación 15, en donde las entidades que comprenden el ámbito se definen por un analista como uno de los dispositivos dentro del servicio en línea (110) o cuentas de usuario del servicio en línea (110).

17. Un dispositivo de almacenamiento legible por computadora que incluye instrucciones ejecutables por procesador para detectar ámbitos comprometidos en un servicio en línea (110), que comprende:

recibir (510) resultados de detección de comportamientos que ocurren en los dispositivos dentro del servicio en línea (110);

puntuar (520) de los resultados de detección basándose en cómo los comportamientos anómalos están dentro del servicio en línea (110), en donde los resultados de detección son puntuados con base en una proporción entre un recuento de subpoblación y un recuento de población para el comportamiento dentro del servicio en línea (110);

excluir los resultados de detección puntuados que tienen uno o más de un recuento de subpoblación y un recuento de población para el comportamiento por debajo de uno o más de un umbral de subpoblación y un umbral de población, respectivamente;

organizar (530) los resultados de detección puntuados restantes de acuerdo con los ámbitos, en donde un ámbito dado está asociado con un dispositivo dado o una determinada cuenta de usuario en el servicio en línea (110);

aplicar (540) la lógica de detección de señales múltiples al ámbito determinado para producir una puntuación de confianza que indica si el ámbito determinado está comprometido;

determinar (550) si alertar a un analista del ámbito determinado que está comprometido en función de comparar la puntuación de confianza con un umbral de alerta; y

en respuesta a la determinación de que el analista va a ser alertado del ámbito determinado que está comprometido, generar y transmitir una alerta (560).

18. El dispositivo de almacenamiento legible por computadora de acuerdo con la reivindicación 17, en donde la puntuación (520) de los resultados de detección además comprende:

- calcular (600) un identificador para un determinado resultado de detección;
- recuperar (620) una cuenta de agregado para el resultado de detección dado;
- incrementar (630) los recuentos de población agregados para el resultado de detección dado;
- calcular (640) una puntuación de anomalía para el resultado de detección dado basándose en los recuentos de población agregados; y

asociar la puntuación de anomalía con el resultado de detección dado para producir un resultado de detección puntuado.

19. El dispositivo de almacenamiento legible por computadora de acuerdo con la reivindicación 17, en donde la organización (530) de los resultados de detección puntuados de acuerdo con los ámbitos además comprende:

- recibir una definición de ámbito identificando una característica a través de la cual se dividen los resultados de detección;
- recibir una ventana de tiempo a través de la cual los resultados de detección se van a analizar;

y

- dividir los resultados de detección que se observaron dentro de la ventana de tiempo en los ámbitos de acuerdo con los valores de la característica identificada incluidos en los resultados de detección.

20. El dispositivo de almacenamiento legible por computadora de acuerdo con la reivindicación 17, en donde la aplicación (540) de lógica de detección de señales múltiples al ámbito determinado para producir la puntuación de confianza además comprende:

- seleccionar (710) un modelo predictivo;
- extraer (720) características de los resultados de detección;
- puntuar (730) las características para la conversión en características valoradas numéricamente; y

proporcionar (740) las características del modelo predictivo para generar la puntuación de confianza.