REIVINDICACIONES

1. Sistema para la autenticación de la identidad de un usuario mediante la implementación de múltiples factores, que consiste en al menos uno de circuitos electrónicos digitales, hardware de computadora, firmware, software o combinaciones de los mismos, caracterizado porque comprende al menos un producto de programa de computadora tangiblemente incorporado o almacenado en un dispositivo de almacenamiento legible por máquina para su ejecución por un procesador programable; uno o varios periféricos de entrada biométrica; y acciones del método pueden ser realizadas por un procesador programable que ejecuta un programa de instrucciones para realizar funciones de la invención operando sobre datos de entrada y generando salida.

2. Sistema de autenticación de acuerdo con la reivindicación 1, caracterizado porque los procesadores adecuados incluyen al menos uno de un microprocesadores de propósito general y especial, la computadora incluirá uno o más dispositivos de almacenamiento masivo para almacenar archivos de datos seleccionados de al menos uno de discos magnéticos, como discos duros internos y discos extraíbles; discos magneto-ópticos; y discos ópticos, en donde los dispositivos de almacenamiento adecuados para incorporar de manera tangible instrucciones y datos de programas de computadora incluyen todas las formas de memoria no volátil, incluidos, a modo de ejemplo, dispositivos de memoria semiconductora, como EPROM, EEPROM y dispositivos de memoria flash; discos magnéticos como discos duros internos y discos extraíbles; discos magneto-ópticos; y discos CD ROM. Cualquiera de los anteriores puede ser complementado o incorporado en ASIC (circuitos integrados específicos de la aplicación).

3. Sistema de autenticación de acuerdo con la reivindicación 1, caracterizado porque Los dispositivos de almacenamiento pueden comprender dispositivos

locales, dispositivos remotos, dispositivos virtuales, o combinaciones de los mismos.

4. Un método para la autenticación de la identidad de un usuario mediante el sistema de las reivindicaciones 1 a 3, caracterizado porque comprende los pasos de:

1. Recibir en el Gestor de Mecanismos de Validación de Identidad una solicitud de validación de cada uno de los canales de contacto y los cuales están configurados. La solicitud es recibida por el micro servicio “RestRequest”, el cual valida los datos enviados conforme a estructura, tipos de datos, datos requeridos.
2. Autenticar la petición utilizando “Jano”.
3. Registrar la información en “Redis” donde se mantendrá esperando la respuesta por el “ID de Request”.
4. Determinar si es una solicitud no iniciada, valida si la transacción y el medio de solicitud existen.
5. Enviar la información del “Request” hacia “Completion” e iniciar el proceso de completitud de los datos de la petición.
6. Llamar a los servicios de completitud externos del Gestor de Mecanismos de Validación de Identidad dentro los que se encuentran:
    I. Apolo = Aplicación usada por un asesor para asistir telefónicamente a los clientes y desde el que se invoca la solución.
    II. Reconocer = Consulta bases de datos externos de burós de crédito.
    III. Catálogo de Transacciones, Canales, Mecanismos
    IV. Test de Identidad = Mecanismo de preguntas reto creado con la información del afiliado.
    V. Cartera = Recurso que permite calificar los clientes preferenciales.
    VI. Calificación de Riesgo = Basada en información financiera del cliente en la organización.
    VII. Azure AD

VIII. Lista restrictiva = Lista compuesta por investigación de Antifraude o información de fuentes externas.

7. envíar los datos de completitud al micro-servicio de “RuleProcessor” que será el encargado de orquestar las reglas para determinar la lista de mecanismos a aplicar al cliente.
8. Determinar, por los datos que se extrajeron en Completitud, más los datos del propio “Request” inicial, y teniendo en cuenta una serie de reglas que se deben cumpli,r la lista de mecanismos a aplicar.
9. determinar las validaciones que el cliente ha pasado en un tiempo determinado
10. realizar las consultas necesarias para completar la información requerida
11. enviar los datos de completitud y la lista de mecanismos a ser aplicados al micro-servicio “ExecuteMechanism”, el cual busca de la lista de mecanismos a aplicar el primero que no haya sido validado y llama el servicio externo al Gestor de Mecanismos de Validación de Identidad que inicia el mecanismo de validación.
12. enviar los datos recolectas más la respuesta de la iniciación del primer mecanismo no válido a “SendResponse”. Este almacena toda la petición en la Base de Datos para posteriores peticiones.
13. insertar los datos en “Redis” donde “RestRequest” está esperando para enviar la respuesta de la petición
14. iniciar una petición de validación del mecanismo iniciado. Se mantiene leyendo de Redis la respuesta.
15. validar que la petición de inicio haya sido ejecuta correctamente y que esté vigente la solicitud
16. envíar a validar el mecanismo, donde es llamado el servicio de validación correspondiente al mismo mecanismo iniciado
17. verificar que la validación haya sido exitosa y se marca el mecanismo como válido en la lista de mecanismos
18. envíar respuesta de mecanismo no válido.

5. Un método para la autenticación de la identidad de un usuario de acuerdo con la reivindicación 4, caracterizado porque el paso de generar una prueba de identidad, el cual sonta de las siguientes etapas:

1. El test de identidad recibe una solicitud proveniente de alguno de los canales de contacto con número de documento.
2. La información inicial recibida se usa para consultar en la tabla de calificación de riesgo, el segmento al que pertenece el afiliado y conocer de esta forma los parámetros que deberán ser usados.
3. Los parámetros consultados según el nivel de riesgo del cliente permiten identificar la cantidad de intentos y fallos por día, mes y año.
4. Posterior al conocimiento de parámetros del afiliado se pasa a buscar la cantidad de ingresos previos realizados, para reconocer si se debe considerar las restricciones establecidas por los parámetros.
5. Con la identidad realizados anteriormente, se indaga en cada una de las sesiones si ha aprobado o reprobado en los intentos.
6. Una vez validado los intentos y resultados se consultan los tres parámetros que concuerdan con el nivel de riesgo del cliente.
7. Los tres parámetros son Acidez, Poder de discriminación y Dificultad. Acidez mide el porcentaje de preguntas reprobadas, Poder de discriminación mide la capacidad de diferenciar que el afiliado sea quien dice ser y Dificultad es definido por el comité de Riesgos y Antifraude, calificando la dificultad de la pregunta de 1 a 5, siendo 1 fácil y 5 difícil.
8. Consultados los parámetros del afiliado, pasa a la tabla de cuestionarios, donde se encuentra enlistado la cantidad de preguntas disponibles para el afiliado y busca el cuestionario que cumpla con los parámetros acordes el nivel de riesgo del cliente.
9. Por último, una vez se ha seleccionado el cuestionario, el programa consulta cual es el porcentaje o calificación mínima para aprobar las preguntas. Cabe aclarar que cada una de las preguntas cuentan con un valor diferente; las preguntas con mayor dificultad tienen mayor valor.

10. El porcentaje de aprobación del cuestionario es parametrizable según el nivel de riesgo de cliente. Es decir que es parametrizable el porcentaje requerido de aprobación.
11. En el caso práctico el afiliado e interesado en realizar la transacción, se le exponen unas preguntas las cuales retorna al mecanismo con las respuestas seleccionados y dependiendo acierto o desaciertos conseguir validar su identidad para continuar con la transacción requerida.