UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE INGENIERÍA

Implementación de Autenticación por Voz en Centro de Contacto

INFORME DE ACTIVIDADES PROFESIONALES

Que para obtener el título de

Ingeniero Mecánico Electricista

Área Eléctrica y Electrónica

P R E S E N T A

Jorge Rubén González Islas

ASESOR DE INFORME

M. en C. Edgar Baldemar Aguado Cruz

Ciudad Universitaria, Cd. Mx., 2020

ÍNDICE

INTRODUCCIÓN

Definición de un centro de contacto:

Un centro de contacto es un sistema basado en un procesador que proporciona enrutamiento de llamadas y contactos para transacciones de telefonía de gran volumen, con estaciones "agentes" de respuesta especializada y un sofisticado sistema de gestión de contactos en tiempo real. La definición incluye todos los sistemas de centros de contacto que proporcionan capacidades de manejo de contactos entrantes y distribución automática de contactos, combinados con un alto grado de sofisticación en términos de gestión dinámica de tráfico de contactos.

Un centro de contacto admite las interacciones de los clientes en una variedad de canales, incluidas llamadas telefónicas, correo electrónico, chat, web, colaboración web y la adopción emergente de interacciones en redes sociales, y es diferente de los centros de llamadas solo de telefonía. Aunque los centros de contacto admiten más de un canal, no necesariamente implican el uso de colas universales. En cambio, pueden admitir múltiples canales pero usan sistemas separados y, en algunos casos, procesos comerciales para hacerlo. Las tecnologías subyacentes clave incluyen la distribución automática de llamadas, la integración de telefonía informática, la respuesta de voz interactiva y los marcadores de salida.

Existen aplicaciones de software que generalmente residen en un servidor adjunto o en un sistema de procesador basado en conmutador, ubicado en las instalaciones de un cliente o en un sitio de terceros. Para enrutar llamadas telefónicas, el sistema que proporciona el control de llamadas puede ser un recurso específico de la aplicación o puede admitir una instalación PBX / distribuidor automático de llamadas de doble función. Las arquitecturas más nuevas admitirán las reglas comerciales de enrutamiento de llamadas del centro de contacto en un "servidor de aplicaciones" que puede dirigir y monitorear llamadas a través de una puerta de enlace de telefonía utilizando SIP u otros protocolos de softswitch. La infraestructura también se puede proporcionar como un "servicio administrado" en el sitio como una solución de "servicio alojado" externa y dedicada; o como una solución de "software como servicio" (SaaS) de recursos compartidos fuera del sitio.

Proporcionan un enrutamiento inteligente de una comunicación entrante (es decir, una llamada, correo electrónico, chat de texto, colaboración web o fax) al recurso apropiado (es decir, asistido por agente o autoservicio) a través de un algoritmo sofisticado.

Brindan la capacidad de generar informes históricos de actividad (que cubren al menos 30 días) y capacidades de supervisión que incluyen, entre otros, monitoreo y generación de informes en tiempo real de la carga de trabajo de un sistema, búsquedas de estado del agente, visualización del número de contactos en el cola, y la capacidad de cambiar el estado del agente.

Los centros de contacto más sofisticados cuentan con un IVR (respuesta de voz interactiva), una opción de procesamiento de voz / llamada para mejorar la funcionalidad e integración del centro de llamadas. Permite a las personas que llaman tener más flexibilidad para acceder a la información mediante dígitos correspondientes a menús y submenús, o dejar mensajes (*Imagen 1*). El uso de esta opción puede "descargar" el volumen de llamadas de los agentes al IVR o mejorar el equilibrio de carga haciendo que los agentes manejen los mensajes grabados durante los períodos lentos. Un número cada vez mayor de desarrolladores de IVR ahora usan el reconocimiento de voz en sus aplicaciones.

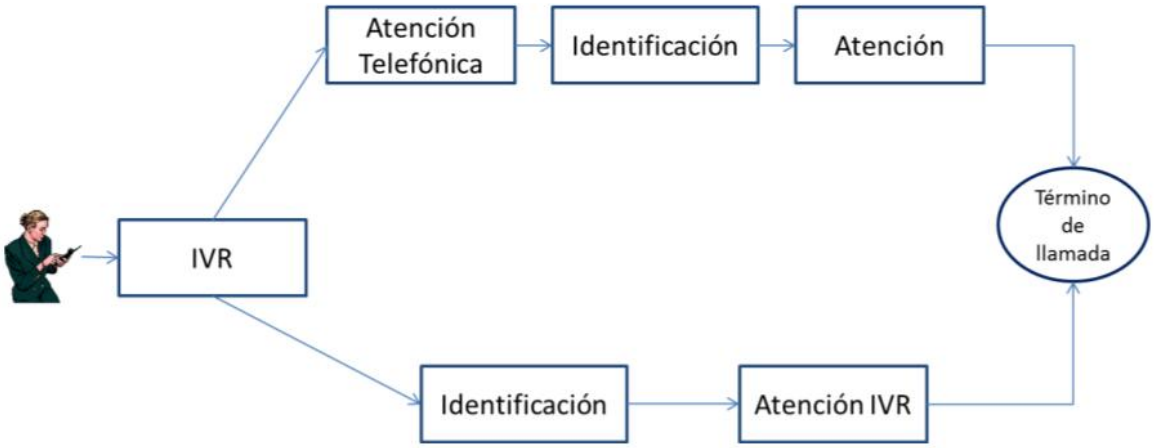

Imagen 1 OPERATIVA DE UN CALL CENTER

La autenticación del centro de contacto está diseñada para identificar el riesgo de las llamadas entrantes, de modo que un banco puede tomar las medidas adecuadas para aceptar o rechazar la llamada en función de sus umbrales comerciales. Todo esto mediante un cuestionario que el ejecutivo realiza para validar que la persona del otro lado del teléfono es quien dice ser. Si bien existen varios métodos de cómo los bancos pueden monitorear las llamadas, algunos expertos creen que todavía hay espacio para crecer cuando se trata de verificar las llamadas para proteger a sus clientes del fraude telefónico.

ALCANCE

Dentro de los servicios de atención existentes en el centro de contacto, la implementación de autenticación mediante el uso de biometría de voz estará enfocada para utilizarla en el centro de contacto y en otros canales de atención, Implementar el mecanismo de autenticación de biometría de voz en la banca telefónica permitirá identificar de forma sencilla la identidad del usuario que está tratando de realizar una operación de forma remota (*Imagen 2*), así como preparar la plataforma para incluir nuevos servicios que permitan implementar la normativa, con este tipo de tecnología.

Con la autenticación por voz se busca mejorar la experiencia y satisfacción del cliente al momento de interactuar con los servicios que incluyan esta tecnología, es decir poder ofrecer la opción de autenticarse con su voz y no pasar por el proceso de cuestionamientos ni recordar contraseñas, disminuyendo el tiempo de duración en la llamada.

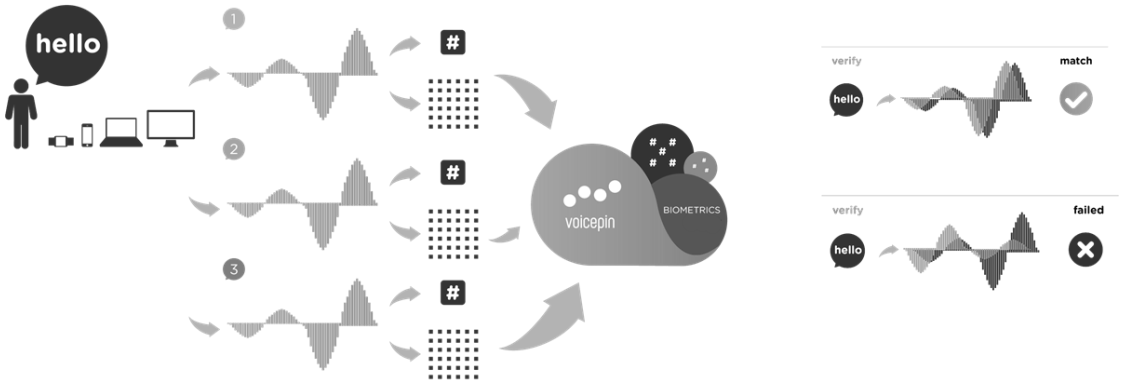

Imagen 2 AUTENTICACIÓN POR VOZ EN UNA LLAMADA

Este tipo de soluciones innovadoras ponen banco a la vanguardia tecnológica, demostrando su solidez en el sector financiero; cabe mencionar que el uso de Biometría por voz será una decisión del cliente para activarla o bien seguir con su autenticación actual por clave de acceso y/o esquema de seguridad.

Al Implementar esta tecnología podremos contar con una mayor eficiencia operativa en la institución al disminuir fraudes por suplantación de identidad por tener una mayor certeza en la identificación de personalidad, haciendo sencillo y rápido el proceso de identificación al tener un Factor 4 de Autenticación, definido en la tabla de la página 18.

OBJETIVO GENERAL

Desde un punto de vista personal, este informe de actividades profesionales además de conseguir obtener el titulo de ingeniero, es una oportunidad de agradecer el gran aporte qué la Universidad y sus profesores me brindaron. El poder utilizar las metodologías, la inducción a la consulta y de alguna forma implementar materias cursadas para el seguimiento y realización de este proyecto y unos tantos mas, en todos su conjunto, me llena de satisfacción el realizarlo y compartirlo.

Desde un punto de vista profesional, el adecuar para el entorno bancario los avances recientes en sistemas para conseguir una autenticación remota fiable y gestión de identidades de sus clientes. Conseguir reducir enormemente costes, estar a la vanguardia con las nuevas tecnologías y principalmente ofrecer una rápida y mejor experiencia al cliente.

OBJETIVOS PARTICULARES

- Fortalecer la Banca Telefónica de la banca.
- Disminución de la suplantación de identidad y los fraudes posibles.
- Incrementar los niveles de seguridad en el proceso de autenticación con Factor 4.
- Generar las firmas biométricas de voz de los usuarios para aprovechar los beneficios de la tecnología.
- Optimizar los tiempos de respuesta.
- Mejorar los tiempos de atención a los usuarios y utilizar el tiempo de los ejecutivos de atención en otras operaciones.
- Automatizar los procesos de autenticación.
- Sustituir los modelos tradicionales y conseguir que los flujos de los procesos se efectúen directamente desde el usuario, utilizando la tecnología.
- Reducir los costos operativos.
- Mejorar la experiencia y servicio a nuestros clientes y usuarios con soluciones innovadoras.
- Obtener información en formato de texto extraída de los archivos de audio de cada cliente para analítica e inteligencia artificial.
- Conversión de voz a datos para utilizarlos en otras plataformas y poder identificar patrones, conductas y hasta para automatizar otras transacciones.

DETALLES DE LA EMPRESA

Historia

El banco fue fundado en 1899 en la ciudad de Monterrey, donde comenzó sus operaciones como un pequeño jugador regional. En 1992, en el proceso de privatización de la banca, fue adquirido por un grupo de empresarios. A través de una serie de adquisiciones estratégicas después de la crisis financiera mexicana a mediados de 1990, el banco consolidó una presencia nacional en México.

Actualmente opera como un grupo financiero, bajo un modelo de banca universal ofreciendo una amplia variedad de productos y servicios a través de su casa de bolsa, las compañías de pensiones y seguros, Afore, sociedades de inversión, así como las empresas de arrendamiento y factoraje y la almacenadora.

1899 Fundación de Banco

1947 Fundación de Banco Regional

1986 Fusión de Bancos

1992 Es adquirido por un grupo de empresarios

1993 Con el propósito de incrementar la oferta de servicios, el banco adquiere una casa de Bolsa

1995 A pesar de la crisis financiera, el banco mantiene su solidez e inicia la incorporación de otro banco, convirtiéndose en una institución multi regional

1997 La institución adquiere un banco más y se asocia con una operadora de fondos de pensión

1998 Inicio de una nueva manera de atender al cliente a través de tecnología informática moderna: el sistema bancario en línea y el centro de atención telefónica

2000 El Grupo Financiero es reconocido por sus valores institucionales y solidez financiera con la categoría “Banco sólido” por la calificadora Fitch Ratings

2001 Adquisición de 100% de las acciones de otro banco

2002 Con la integración del nuevo banco, se consolida como la cuarta red de sucursales más importante del sistema bancario mexicano

2003 El banco se suma a las tendencias de globalización y forja alianzas que fomentan el crecimiento económico de México

2004 Fortalecimiento y enfoque en estrategias de crecimiento con la generación de productos y servicios novedosos

2005 Alianza con Telecomm - Telégrafos para bancarizar a miles de mexicanos. Reubicación de la oficina matriz del grupo en un moderno edificio corporativo en Santa Fe, ciudad de México

2006 El banco cruza fronteras con la adquisición de Inter National Bank y la remesadora Uniteller en Estados Unidos

2007 El banco cuenta ya con más de mil sucursales y de 3,500 cajeros automáticos. Adquisición de la remesadora Motran de California, Estados Unidos

2008 Es nombrado “Mejor banco de México” y “Mejor banco de Latinoamérica” por la revista Euromoney

2009 Obtiene por quinta ocasión la distinción de “Mejor banco del año en México” por la revista especializada The Banker

2010 World Finance lo reconoce como “El mejor grupo financiero de México 2010”

2011 Es uno de los tres finalistas para el reconocimiento de “Sustainable Bank of the Year 2011”, otorgado por Financial Times y el IFC

Nueva fusión del banco con otra banca, lo que la convierte en la tercera institución bancaria de México

2012 Inauguración del Centro de Contacto.

Creación de 5 Consejos Regionales, con el objetivo de brindar asesoría al Presidente del Consejo de Administración sobre aspectos relevantes y oportunidades en las diferentes zonas del país

2013 Se convierte en la mayor administradora de fondos para el retiro en el país, después de concretar la adquisición de una gran Afore

2014 Nueva Presidencia del Consejo de Administración y Dirección General de Grupo Financiero

2015 Inicia el programa de transformación que tiene como objetivo mejorar la propuesta de valor para nuestros clientes, incrementar la venta cruzada, mejorar los indicadores de rentabilidad y eficiencia y fortalecer la gestión de riesgos

Nace el programa Visión 20/20, en el que busca conseguir duplicar sus utilidades para el año 2020

2017 Se convierte en la primera institución bancaria de México y América Latina en aliarse con PayPal, ofreciendo la posibilidad de tener acceso a 17 millones de comercios en todo el mundo que usan la plataforma digital

El banco refuerza el área de innovación tecnológica buscando conseguir alternativas que resuelvan bajo una buena experiencia los requerimientos de los usuarios

Nuevamente se fusiona con otra banca y busca consolidarse como el grupo financiero numero 2 a nivel nacional

Actualmente da servicio a más de 13 millones de clientes en el sector bancario en todo el país, a través de una red de más de 1,200 sucursales, más de 7 mil cajeros automáticos, más de 5,300 corresponsalías y más de 162 mil terminales punto de venta

Misión: Generar confianza y fortaleza financiera para todos nuestros clientes

Visión: Ser un gran aliado para crecer fuerte con México

Valores: Solidaridad, Innovación, Lealtad, Respeto, Responsabilidad

DESCRIPCIÓN DEL PUESTO

Dentro de este Grupo Financiero, el que redacta este Informe se desempeña como Especialista de Innovación y Transformación Tecnológica. Área en la que busca para los canales de servicio adoptar, diseñar y generar un cambio muy importante y determinante de las herramientas que ayudarán al usuario a efectuar operaciones que conviertan cada transacción en una experiencia sencilla, segura, práctica y más eficiente para la institución.

Actualmente, líder del proyecto de implementación de autenticación por voz (biometría de voz) multicanal, líder de la migración de objetos del cliente al repositorio único de la institución y consultor interno de la implementación de solución de originación de clientes en dispositivos móviles, visor de nuevos proyectos enfocados a la inteligencia artificial y analítica de datos, así como participante en el nuevo proyecto que será la banca por voz.

MARCO TEÓRICO

La autenticación biométrica es la práctica de reconocer y verificar la identidad de una persona a través de un rasgo físico o de comportamiento único como la forma en que una persona habla, o el patrón único de sus huellas dactilares u ojos. Una vez limitado a la ciencia ficción y las películas de espionaje, la biometría de hoy y las tecnologías de autenticación son altamente sofisticadas, seguras y cada vez más ordinarias.

Hoy, cientos de millones de consumidores usan datos biométricos autenticación todos los días, para desbloquear sus teléfonos inteligentes y acceder a sus aplicaciones móviles favoritas a través de escáneres de huellas digitales incorporados en su dispositivos móviles. No solo los fabricantes de dispositivos están adoptando la tecnología. Proyectos de investigación que el mercado mundial de biometría excederá los $ 30 mil millones por 2021, con compañías bancarias y de finanzas personales liderando el cargo.

Según el New York Times, muchos bancos ya están por delante de la curva.

Frente al fraude de documentos y al robo de identidad, con nuevas amenazas como el terrorismo o la delincuencia informática, y frente a los cambios comprensibles en las reglamentaciones internacionales, se están implementando nuevas soluciones tecnológicas gradualmente. Una de esas tecnologías, la biometría, se ha establecido rápidamente como el medio más pertinente para identificar y autenticar individuos de una manera rápida y confiable, a través del uso de las características biológicas únicas.

Hoy, muchas aplicaciones usan esa tecnología. En el pasado, estaba reservada para aplicaciones sensibles, como la seguridad de los sitios militares, sin embargo, ahora se está desarrollando rápidamente, a través de aplicaciones de dominio público.

Adoptar un enfoque multimodal permite una gran seguridad de paso en flujos de trabajo. Por ejemplo, un escaneo rápido de huellas dactilares en una aplicación de banca móvil podría permitir a un cliente acceder al saldo de su cuenta o realizar otras funciones de administración de cuentas de bajo nivel, pero una solicitud para transferir dinero, pagar facturas o solicitar una línea de crédito podría desencadenar una solicitud de iris o autenticación por voz que son mas seguras.

En la biometría de voz hay dos enfoques.

Puedes grabar una frase fija (una muy popular es "mi voz es mi banco") unas cuantas veces, y esa "huella de voz" se usa para compararla con la tuya cuando llamas.

Este método de contraseña fija tarda sólo 1,5 segundos en autenticar.

A otro enfoque lo llaman "expresión libre": mientras sostienes una conversación natural con el centro de llamadas, el sistema chequea que efectivamente eres tú y, unos segundos después, le informa al representante del servicio al cliente que ha verificado su voz o le pide que hagan controles más tradicionales en caso contrario.

Este método de "expresión libre" ha llegado a ser posible en una escala mucho mayor gracias a la creación de mejores algoritmos que analizan las voces con más detalle.

Características físicas, tales como la longitud de tu lengua y el grosor de tus cuerdas vocales y entre otras características, contribuyen a la singularidad de la voz. Además están los rasgos de la personalidad: el tono y la forma en la que pronuncias ciertas sílabas y palabras.

Los algoritmos informáticos de punta pueden analizar cientos de variables y llegar a una autentificación muy segura en cuestión de algunos pocos segundos.

El emplear cualquier elemento corporal con fines de autenticación, va a requerir ser preciso analizarlo y descomponer las diferentes características que forman parte del mismo para, así, poder establecer las diferencias necesarias entre elementos de diferentes personas.

Los sistemas sonoros están formados por ondas periódicas generadas por la vibración de las cuerdas vocales. La frecuencia de estas ondas va a determinar el tono de la voz, y se trata de un sonido estable a corto plazo y de elevada energía.
El espectro de un sonido sonoro se encuentra formado por la envolvente y por las componentes armónicas que son las que forman la estructura fina del espectro.

Los sonidos sordos se producen por constricciones en el tracto vocal. Se trata de sonidos de cierta estabilidad a corto plazo, alta frecuencia y de baja energía.

El espectro de un sonido sordo carece de componentes armónicas.

El hecho de que se puedan generar diferentes sonidos va a ser consecuencia del carácter que presentan lo que se conoce como formantes. Los formantes se corresponden con todo aquello referente a la configuración de los órganos específicos del tracto vocal que se encargan de producir un sonido.

Cada uno de estos sonidos diferenciados van a presentar una envolvente espectral específica que va a permitir diferenciarlos entre ellos, y que va a ser precisamente lo que empleen los sistemas de reconocimiento del locutor.

Por otro lado, la estructura fina del espectro no aporta información relevante ni de utilidad para ser empleada por este tipo de sistemas.

Por lo anterior, la envolvente espectral (*Imagen 3*)., es aquella que va a contener la información útil que permitirá diferenciar la voz de una persona u otra.

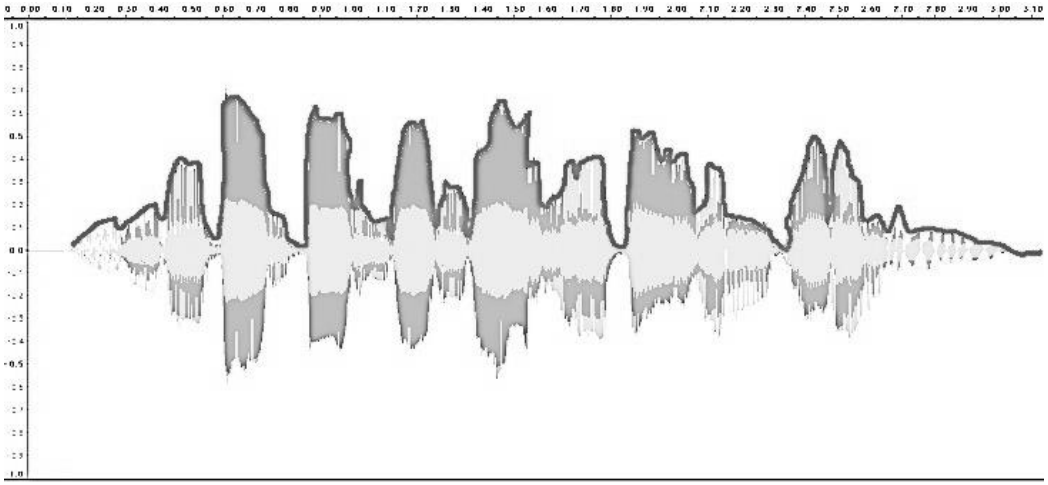

Imagen 3 ENVOLVENTE ESPECTRAL

Los aspectos a los cuales atiende un sistema de reconocimiento biométrico a la hora de diferenciar entre las diferentes voces no difiere en gran medida de aquellos que tiene en cuenta una persona para lograr el mismo fin, con la diferencia de que el sistema de reconocimiento es consciente de ello (porque así se le ha ordenado), mientras que una persona atiende a estos aspectos de forma inconsciente.

Estos aspectos pueden ser clasificados en dos categorías:

1. *Información de bajo nivel*: todos aquellos factores que tienen que ver con el sonido de la voz como consecuencia del tamaño y forma de los órganos encargados de la fonación, resonancia, amplitud de banda, frecuencia de onda, la forma en que se concatenan los sonidos que forman las palabras, entonación en el habla o la duración de los silencios.
2. *Información de alto nivel*: todos aquellos factores que tienen que ver con el dialecto empleado, la jerga, la velocidad al hablar, el léxico, el estilo, o el uso de palabras peculiares.

Sin embargo, la voz humana va a presentar una serie de pequeños inconvenientes al ser empleada como seña de identidad en una identificación biométrica, y es que, con el paso del tiempo, esta se va viendo modificada de manera inevitable; es posible modificar algunos parámetros a voluntad dentro de unos límites; o es posible que debido a determinadas circunstancias (afonía, estado anímico, consumo de sustancias) esta se vea modificada.

Los sistemas biométricos de reconocimiento del locutor van a poder trabajar en tres modos distintos:

a. *Modo de aprendizaje o entrenamiento*: se trata de un modo de trabajo en el cual el

sistema capta la voz de una persona y/o frase en repetidas ocasiones con el fin de analizar todos los factores posibles característicos de la misma. Toda la información recopilada es almacenada en la base de datos del dispositivo y es asociada a la persona que ha efectuado las locuciones.

b. *Modo de trabajo*: en este modo de trabajo el dispositivo capta la voz de un individuo, la analiza, y compara los factores característicos obtenidos con todos los pertenecientes a los individuos almacenados en la base de datos hasta encontrar aquel que coincide con la persona que se encuentra frente al dispositivo y, así, validar la identificación.

c. *Modo de actualización/aprendizaje*: gracias a este modo de trabajo, el sistema será capaz de actualizar la información asociada a la voz de cada individuo y, así, poder modificar todos los factores que se van viendo alterados por el paso del tiempo.

Algoritmos empleados para realizar la identificación por voz.

Como es habitual en este tipo de dispositivos, su funcionamiento está basado en una serie de algoritmos que se encargan de procesar la información y transformarla en datos clasificables y comparables entre sí.

Dependiendo del fabricante del dispositivo se empleará un algoritmo distinto, pero todos ellos se pueden agrupar en tres tipos diferenciados,

Algoritmo de alineamiento temporal dinámico.

Ya se ha comentado en varias ocasiones que es muy improbable que una misma persona pronuncie una misma frase exactamente igual en dos ocasiones distintas.

Estos algoritmos se basan en analizar dos frases enteras e iguales, pero efectuadas en momentos diferentes, dividiéndolas en pequeños fragmentos (del orden de milisegundos), y estableciendo así un alineamiento temporal entre ambas frases.

Una vez efectuado este alineamiento, se calcula la distancia mínima entre cada una de sus características.

El valor de esta distancia es el que validará, o no, la verificación de la identidad del locutor.

Este tipo de algoritmos presentan el inconveniente de que se requiere recitar siempre la misma frase, por lo que actualmente ha caído en desuso.

Algoritmo de redes neuronales.

El principio de funcionamiento de este tipo de algoritmos es el de emular al cerebro humano.

Existen dos tipos diferentes:

1. *Clasificación directa*

El algoritmo busca extraer toda aquella información que sea capaz de discriminar entre locutores y, de esta forma, durante la fase de entrenamiento del sistema, se efectuará una discriminación del locutor que se va a añadir a la base de datos frente al resto de locutores almacenados en ese momento. (*Imagen 4*).

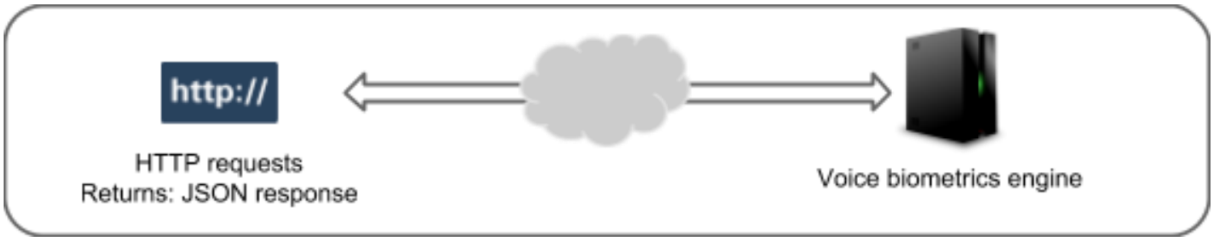

Imagen 4 INTERACCION DE WEB SERVICE CON EL MOTOR BIOMÉTRICO DE VOZ

Este tipo de algoritmo presenta el inconveniente de que conforme va aumentando el número de usuarios almacenados, más trabajo supone este proceso.

2. *Modelado predictivo del locutor*

En este caso se emplean las redes neuronales para realizar un proceso predictivo de producción de voz para los diferentes locutores que se encuentran en la base de datos del dispositivo.

Este proceso predictivo se basa en realizar un entrenamiento de máxima verosimilitud, el cual estima que cada uno de los factores que caracterizan la voz de una persona sigue una distribución normal, asignando a cada uno de ellos la probabilidad de pertenecer a un locutor.

Esto implica crear un modelo independiente para cada locutor, sin tener en cuenta al resto, algo que simplifica el proceso de añadir o quitar usuarios en la base de datos.

Con algunos algoritmos importantes, las voces de cada usuario almacenadas en la base de datos son sometidas periódicamente a una reestimación de sus parámetros.

De esta forma, cada usuario del sistema cuenta con su propio conjunto de datos de entrenamiento, el cual se ve actualizado constantemente.

El modo principal de trabajo de un dispositivo de autenticación por voz se basa en comparar un audio registrado en un momento, con una serie de audios de usuarios almacenados en una base de datos.

Este número de audios de usuarios almacenadas puede llegar a ser, en ocasiones, bastante grande, por lo que establecer una comparación con todas ellos puede volverse un proceso bastante largo que empeoraría la experiencia del usuario.

Para simplificar este proceso, durante la fase de entrenamiento del sistema en la cual se va a registrar un nuevo usuario, este selecciona, de entre todos los usuarios almacenados hasta ese momento, una clasificación, es decir, una selección de aquellos usuarios con características similares al que se va a añadir en ese momento.

De esta forma, durante la fase de trabajo, el sistema realizará una comparación entre el individuo a verificar y clasificar, la cual estará compuesta entre uno y cinco locutores.

ANTECEDENTES DEL PROYECTO, TEMA O PROBLEMÁTICA

Durante un semestre el centro de contacto del banco atendió más de 30 millones de llamadas de entrada, de las cuales el 30% fueron canalizadas con un ejecutivo, teniendo 1.35 min. de tiempo para autenticar al cliente en promedio. Actualmente se utiliza un factor categoría 1 y 2 de seguridad, mediante aplicación de cuestionarios y la utilización de números de identificación personal (NIP).

De acuerdo a la Circular Única de Bancos Artículo 310 se confirman en el siguiente cuadro los diferentes factores de seguridad a utilizar:

CATEGORÍA	CARACTERISTICAS
Categoría 1: Cuestionarios de Seguridad.	No podrán componerse únicamente de datos incluidos en comunicaciones impresas o electrónicas.
Categoría 2: Clave de Acceso, NIP, contraseñas.	La longitud deberá de ser de 6 caracteres a excepción de: Pago Móvil 5 caracteres. Banca por Internet 8 caracteres. NIP ATM / TPV 4 caracteres. No aplican para dicha categoría los siguientes: Identificador de usuario. Nombre de la institución. Más de dos caracteres idénticos en forma consecutiva. Más de dos caracteres consecutivos numéricos o alfabéticos.
Categoría 3: Información contenida o generada por medio o dispositivos electrónicos / Token.	Características de la información generada por el dispositivo: Contar con propiedades que impidan su duplicidad o alteración. Que no pueda ser utilizada en más de una ocasión. Vigencia que no exceda de 2 minutos. No conocida con anterioridad a su generación ya a su uso por funcionarios de la institución.

Categoría 4: Información del usuario derivada de sus propias características.	Características del usuario: Huellas dactilares. Geometría de la mano. Voz. Patrones de Iris o retina, entre otras. Las instituciones que utilicen los factores de autenticación de esta categoría, deberán aplicar la información obtenida por dispositivos biométricos: Elementos que aseguren que la información sea distinta cada vez que sea generada, a fin de que sean contraseñas de un solo uso. En ningún caso podrán utilizarse nuevamente o duplicarse con la de otro usuario.

El volumen de llamadas se ha incrementado de manera importante en los últimos años, y se estima que esta tendencia se conserve o aumente en los próximos, ya que la estrategia de negocio plantea incrementar el número de productos y servicios por cliente para mejorar las cifras de colocación y captación del Banco.

El centro de contacto cuenta con una plantilla de aproximadamente 2,000 ejecutivos y reporta 5.2 millones de llamadas mensuales de Entrada (inbound), en promedio se tiene 5.7 minutos en la duración de llamadas en donde 1.35 minutos son utilizados en el proceso de autenticación, siendo el proceso largo y tedioso para el cliente con el constante uso de preguntas y respuestas o bien con la memorización de claves telefónicas, dado que actualmente la identificación que utilizamos es por clave de acceso.

Debido a la necesidad de optimizar el proceso para atender a los clientes en forma telefónica, se buscaron opciones para reducir estos tiempos, encontrando en el mercado la solución de autentificación basada en biometría de Voz, ya que es considerada como un patrón de identificación único para cada individuo, semejante al uso de las huellas dactilares o el iris, este método se está popularizando, cada día más debido a que permite identificar correctamente al usuario desde la llamada telefónica.

Esta solución ha tomado popularidad para proteger los centros de contacto los cuales han sido objeto de ataques, debido a que la mayoría de los bancos solo se han enfocado en proteger los esquemas de banca móvil y banca por internet. Además que los mecanismos como cuestionarios para verificar la identidad son fácilmente vulnerados por la facilidad de los defraudadores de conseguir documentos con información del cliente, ofrecen una mala experiencia al cliente e influyen en el tiempo de atención. (*Imagen 5*).

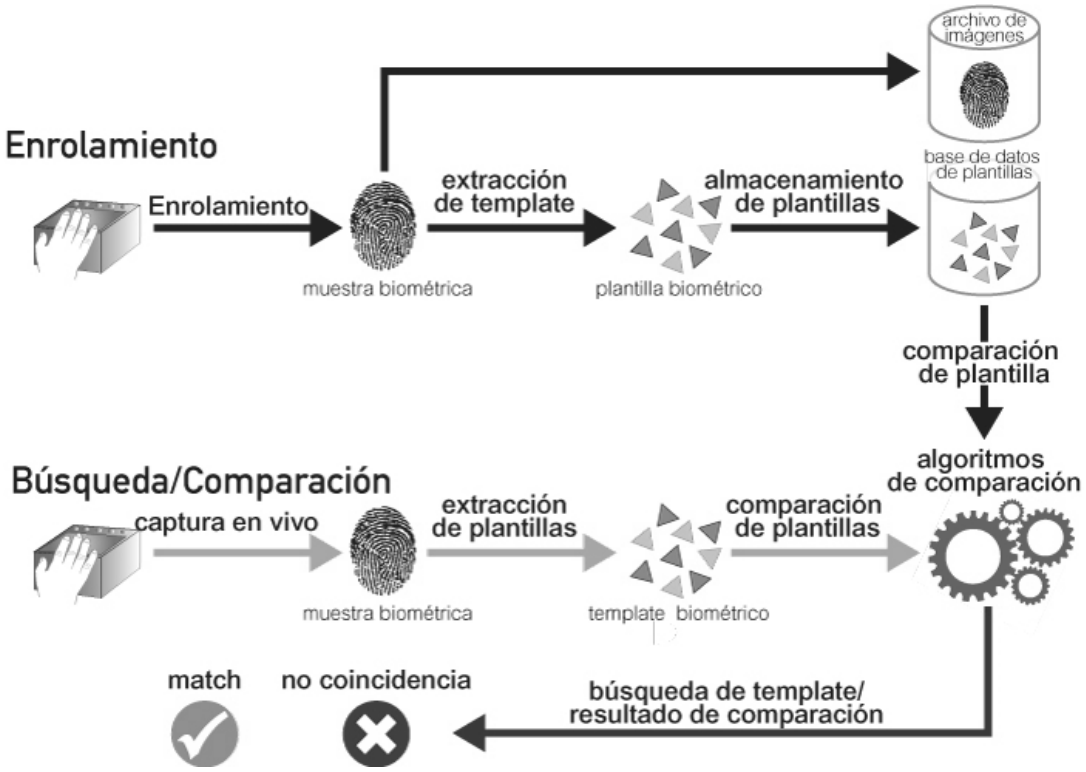

Imagen 5 AUTENTICACION BIOMÉTRICA

Dentro de los servicios de atención existentes en Grupo Financiero, la implementación de autenticación mediante el uso de biometría de voz estará enfocada para utilizarla en el Call Center y en otros canales de atención, el Implementar el mecanismo de autenticación de biometría de voz en la banca telefónica permitirá identificar de forma sencilla la identidad del usuario que está tratando de realizar una operación de forma remota, así como preparar la plataforma para incluir nuevos servicios que permitan implementar la Normativa, con este tipo de tecnología.

Con la autenticación por voz se busca mejorar la experiencia y satisfacción del cliente al momento de interactuar con los servicios que incluyan esta tecnología, es decir poder ofrecer la opción de autenticarse con su voz y no pasar por el proceso de cuestionamientos ni recordar contraseñas, disminuyendo el tiempo de duración en la llamada.

Este tipo de soluciones innovadoras ponen a Grupo Financiero a la vanguardia tecnológica, demostrando una vez más su solidez en el sector financiero; cabe mencionar que el uso de Biometría por voz será una decisión del cliente para activarla o bien seguir con su autenticación actual por clave de acceso y/o esquema de seguridad.

Al Implementar esta tecnología podremos contar con una eficiencia operativa en la institución al disminuir fraudes por tener una mayor certeza en la identificación de personalidad, haciendo sencillo y rápido el proceso de identificación al tener un Factor 4 de Autenticación.

Eficiencia en los tiempos de duración de la llamada, actualmente el total de la llamada es de 5.30 minutos en donde el tiempo de autenticación es de 1.35 minutos, lo cual se estima tener una reducción de 1 minuto por llamada, actualmente se reciben 5.7 millones de llamadas mensuales.

Factores Críticos de Éxito

La solución debe ser capaz de cumplir con los siguientes requerimientos:

- Fácil proceso de enrolamiento.
- Poder tener autenticación por voz en IVR como en atención con Ejecutivos.
- Fiabilidad en el proceso de autenticación del 90%.
- Extracción de Reportes en línea para conocer el comportamiento de la herramienta.
- El sistema deberá tener la capacidad de identificar grabaciones y dispositivos electrónicos de suplantación durante la autenticación.
- La implementación de la herramienta deberá considerar instalación y parametrización para el uso óptimo del servicio.

Se deberá ajustar el contrato Clausulado físico para que de referencia al nuevo proceso de autenticación por Biometría de voz.

Se le deberá informar al cliente en sus estados de cuenta que el contrato clausulado tuvo una modificación. De acuerdo a la resolución publicada en el diario oficial el 3/julio/2013 en la guía para el uso de banca electrónica se establecen cambios en los mecanismos aprobados para ofrecer servicios monetarias en banca telefónica.

Resolución 3/julio/2013 Diario Oficial

http://www.dof.gob.mx/nota_to_doc.php?codnota=5301066&ei=sTInU6v0H8Wa2AWauIHACQ&usg=AFQjCNFg0etLKTHVeE1zaLZ-e-EeYPetFg&sig2=MKFBJH0GQDhXLu8eoxFZQQ&bvm=bv.62922401,d.b2I

Resolución 15/enero/2010 Diario Oficial

http://www.dof.gob.mx/nota_detalle_popup.php?codigo=5129441

SUPUESTOS

El proyecto permitirá al centro de contacto contar con la autenticación de los clientes mediante la Voz, generando una mejor experiencia al cliente y facilitando procesos internos.

La herramienta deberá permitir la autenticación mediante el IVR y mediante la atención de ejecutivos.

El proceso de enrolamiento deberá ser incluido en la implementación de este proyecto.

La herramienta podrá ser utilizada en cualquier proceso interno del banco que requiera la categoría 4 de autenticación.

La validación del entregable final deberá cumplir en su totalidad con los objetivos planteados del requerimiento en cuestión, cualquier desviación a los objetivos del presente requerimiento deberá ser notificada al solicitante para que se realice el ajuste correspondiente.

Todas las operaciones de este requerimiento tanto las exitosas como las no exitosas deberán grabarse (log transaccional, host o donde el área de Tecnología determine y que puedan ser consultados por el negocio) con todo el detalle del paso a paso de la operación, si se marca algún error, quedará registrado este error, si el cliente cancela en algún paso la transacción se mostrará este detalle en los repositorios correspondientes, adicionando el tiempo que le tomó al usuario decidir la opción durante la llamada.

Usuario marca al centro de contacto y recibe bienvenida; accede al menú principal; si el servicio requiere de atención de un ejecutivo, se le transfiere a el, identifica si el cliente esta enrolado o no, de estar enrolado, se efectúa la autenticación por freespech (pasivo) y se ofrece el servicio, caso contrario se atiende de forma tradicional. Si el servicio no requiere de atención de un ejecutivo, se sigue el menú del IVR y en el que se solicita identificar, de estar enrolado se solicita frase de autenticación y de ser valida, se ofrece el servicio; en caso de ser un cliente no enrolado, se le invita a enrolar y de estar todo correcto se le atiende a la transacción solicitada (*Imagen 6*).

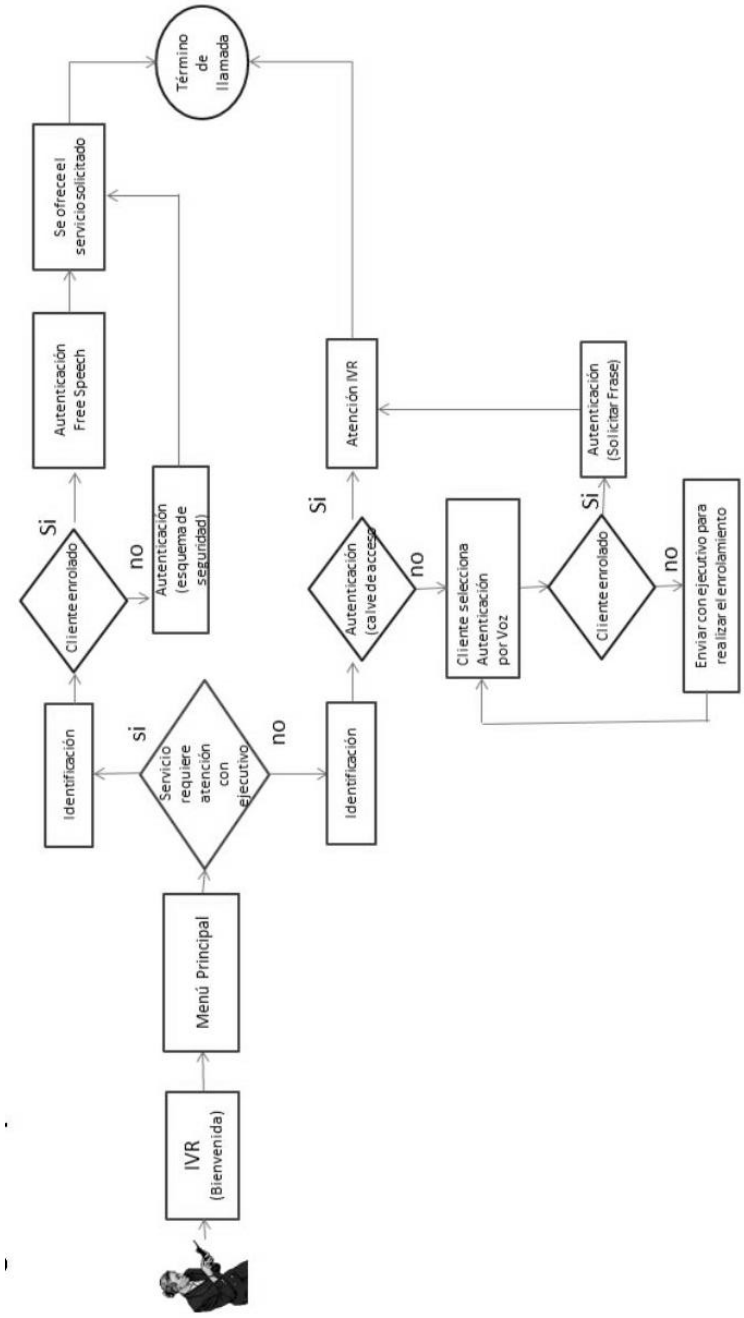

Imagen 6 OPERATIVA ESPERADA CON AUTENTICACIÓN POR VOZ

Debe considerarse que las transacciones nuevas deben ser incluidas en los reportes que se entregan al área de la rentabilidad para la generación del estado de resultados y cada interacción con algún aplicativo central deberá ser tomada en cuenta.

Todas las leyendas del proyecto tanto de errores como de funcionalidades deberán ser definidas durante el desarrollo de cada requerimiento.

Todas las leyendas del proyecto tanto de errores como de funcionalidades deberán poder definidas durante el desarrollo de cada requerimiento y deberán ser parametrizables en la consola central de negocio para poder ser cambiadas sin necesidad de un requerimiento tecnológico.

La consola central de negocio deberá permitir la explotación de las estadísticas de las operaciones de este requerimiento bajo el criterio de Cliente, Transacción, Día, Mes, Hora, Geolocalización, segmento, etc.

El detalle de los reportes que serán explotados por la consola central se encontrará en el requerimiento de reportes de transaccionalidad en Contact Center, adicionando a los reportes el criterio de mostrar el tiempo que le tomó al usuario decidir en cada opción dentro del IVR e identificando plenamente el comportamiento del cliente durante la llamada.

DEFINICIÓN DEL PROBLEMA O CONTEXTO DE LA PARTICIPACIÓN PROFESIONAL

Identificar las mejores aplicaciones de autenticación por voz en el mundo, que consideren el idioma español y que tenga la posibilidad de adaptarse a la Arquitectura Multicanal (MCA) Implementada previamente en el banco, y que de igual forma se defina una Arquitectura de Seguridad también Multicanal.

Considerar para la evaluación que todos los métodos de reconocimiento biométrico existentes tienen sus ventajas e inconvenientes, desde la voz y la escritura, hasta el iris y los patrones de venas de la mano. Comparar unos rasgos biométricos con otros en cuanto a su seguridad, habría que especificar un modelo de atacante que caracterice preguntas como: ¿cómo se produce el ataque?, ¿cuánto le cuesta al atacante conseguir el éxito en su ataque? La idoneidad de un rasgo biométrico u otro dependerá de la aplicación en cuestión, del escenario de uso, del modelo de atacante que quiere vulnerar el sistema, y de los recursos que disponga para ello.

Comparar un rasgo biométrico u otro en base a otros factores como usabilidad, coste económico, durabilidad, etc.

Todos estos factores, una vez determinada la aplicación y escenario, son los que harán que un rasgo biométrico u otro, o una combinación de varios, utilizados de una forma concreta y con unos sensores determinados, sea la solución óptima.

Dada la inversión realizada previamente por el banco en productos de Seguridad de Oracle, se tomó la decisión de implementar la Arq. de Seguridad de forma Independiente de IBM.

El esquema de seguridad original utilizado el banco, basado 100% en OAM-OID, tiene limitantes.

El proyecto inicia identificando y recopilando los requerimientos para soportar una Arquitectura de Seguridad Multicanal.

De la misma forma, se enlistan los siguientes requerimientos que se deben de cumplir para considerar alguna aplicación:

1. Permitir a los usuarios seleccionar y usar una o cualquiera de las múltiples formas de métodos o esquemas de identificación.

    - Ej. Los usuarios podrán introducir ID de usuario, número de cliente, número de cuenta, número de tarjeta, Foto Personal, etc. Y en donde aplique.

2. Permitir a los usuarios seleccionar y utilizar alguno de los métodos o esquemas de autenticación disponibles.

    - Los métodos de autenticación no estarán necesariamente ligados a un método de identificación.

    - Los métodos de autenticación disponibles, dependerán de la capacidad del canal y el enrolamiento de los usuarios.

3. Extensible, proveer la capacidad de integrar nuevos métodos de identificación y autenticación.

    - Los nuevos métodos de autenticación se integrarán con cambios menores en la arquitectura de seguridad, usando plugins o conectores proporcionados por los fabricantes, o mediante desarrollo interno.

4. Desacoplamiento de las aplicaciones de canal.

    - Permitir la integración de nuevos métodos de identificación o autenticación, sin requerir necesariamente que las aplicaciones de cada canal sean modificadas o actualizadas. El desacoplamiento puede ser total o parcial.

5. Capacidad real multicanal.

    - Proveer soporte para aplicaciones Web, Ajax/Web2.0/Rich, Portal / portlets, móvil, IVR, ATM (Multivendor).

    - Debe soportar el uso de servicios web basados en arquitecturas SOA para integración de otros canales.

6. La Autorización Adaptativa deberá acceder a los servicios de recursos y de la interfaz de usuario o del back-end.

    - El acceso a los recursos o servicios de back-end, se autorizará mediante la evaluación del nivel de seguridad proporcionado por el método de autenticación utilizado, la puntuación de riesgo de la sesión, y el nivel de seguridad necesario para acceder al recurso o servicio. Las respuestas posibles son : permitido, bloqueado o "permisos insuficientes”.

7. Deberá ser capaz de manejar una definición declarativa de roles / grupos, recursos, servicios, niveles de seguridad y permisos. (*Imagen 7*).

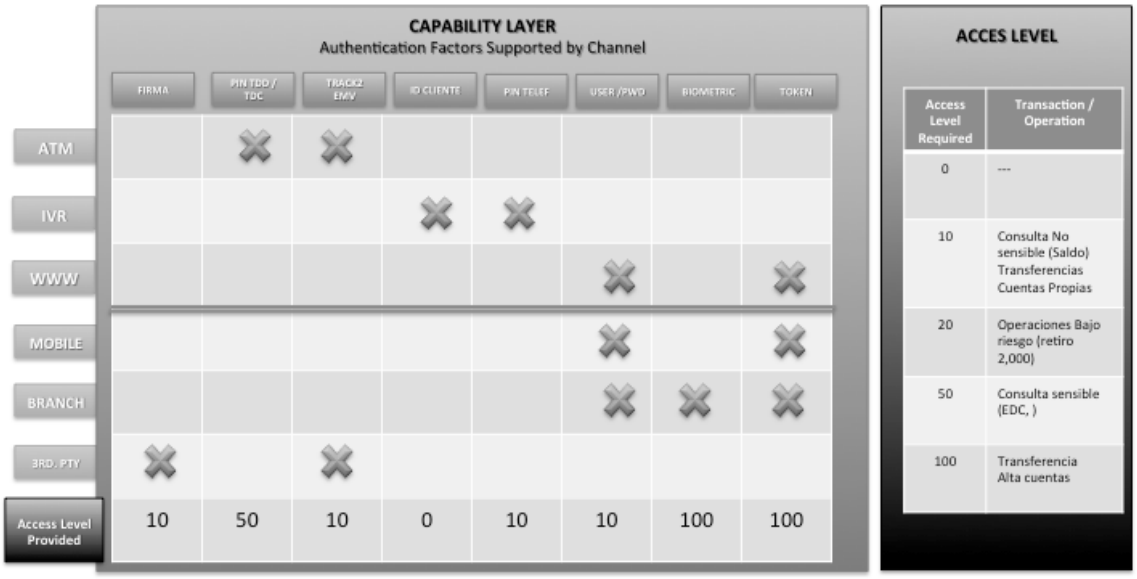

Imagen 7 DIMENSIONES DE SEGURIDAD

8. No habrá necesidad de modificar la arquitectura o iniciar nuevos proyectos de desarrollo.

9. Control de acceso por perfiles de usuario.

10. Consolas de gestión (configuraciones, reglas dinámicas, perfiles y niveles de seguridad). (*Imagen 8*).

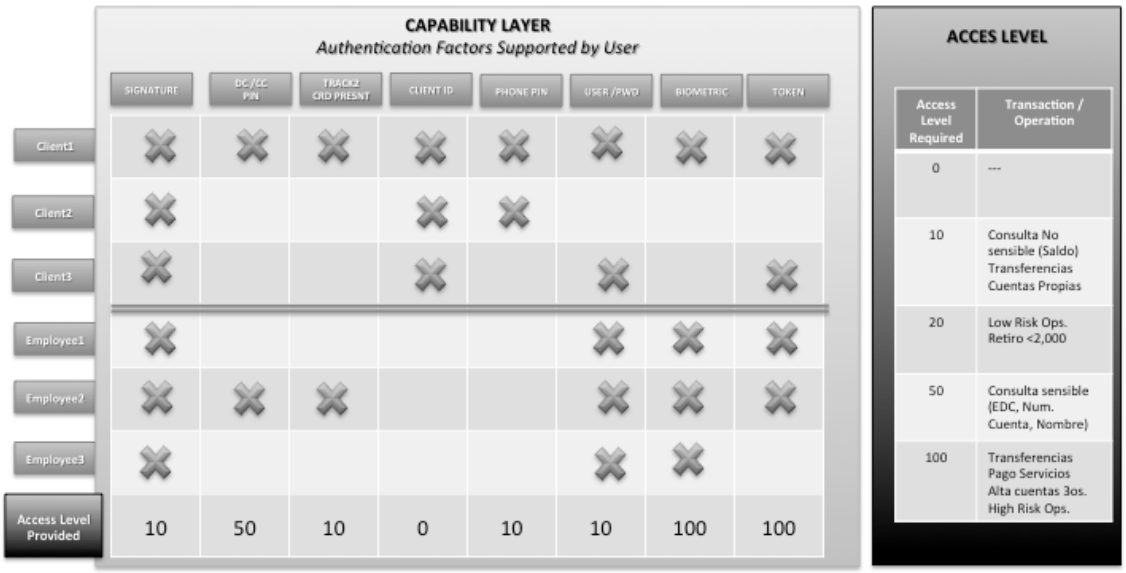

Imagen 8 FACTORES DE SEGURIDAD

11. Asignación de niveles de seguridad a grupos de servicios.

12. Motor de Reglas Avanzado (AbInitio).

13. Integración con WMBTT.

14. Soportar múltiples dimensiones de Seguridad: Cliente, Usuario Interno y Dispositivo.

Que en el futuro, la aplicación sea capaz de adaptarse a la capa de seguridad multicanal. (*Imagen 9*).

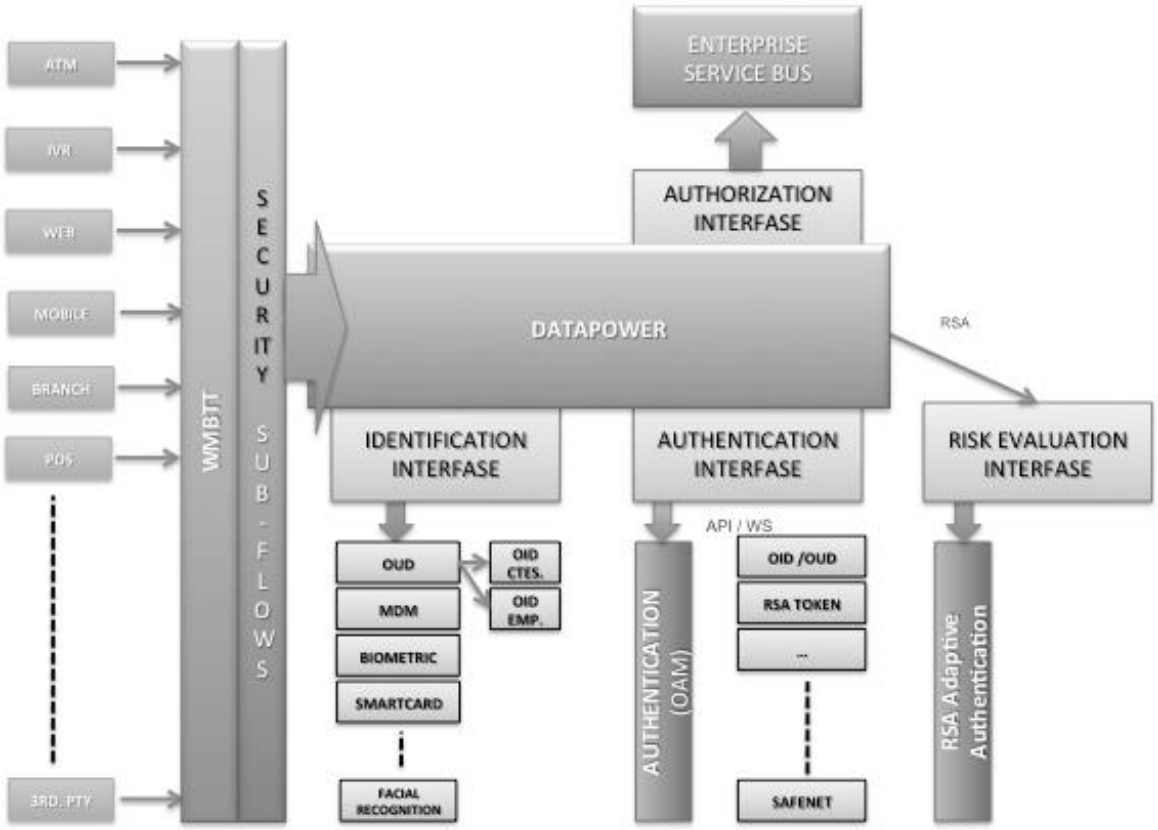

Imagen 9 CAPA DE SEGURIDAD MCA

Basándonos en todo lo anterior y buscando con las diferentes opciones, se consiguió que solo 2 de los proveedores de aplicaciones, cumplieran técnicamente con estos requisitos. De acuerdo a los procesos internos, se eligió a uno de ellos.

El proveedor elegido y después de varias sesiones técnicas para entender los requerimientos de la aplicación y a la vez dar a conocer los detalles de la arquitectura MCA del banco, se llegó a definir la siguiente arquitectura a integrar (*Imagen 10*):

Misma que se evaluó dentro del proceso de análisis técnico y que por lo cual se definió el hardware a utilizar.

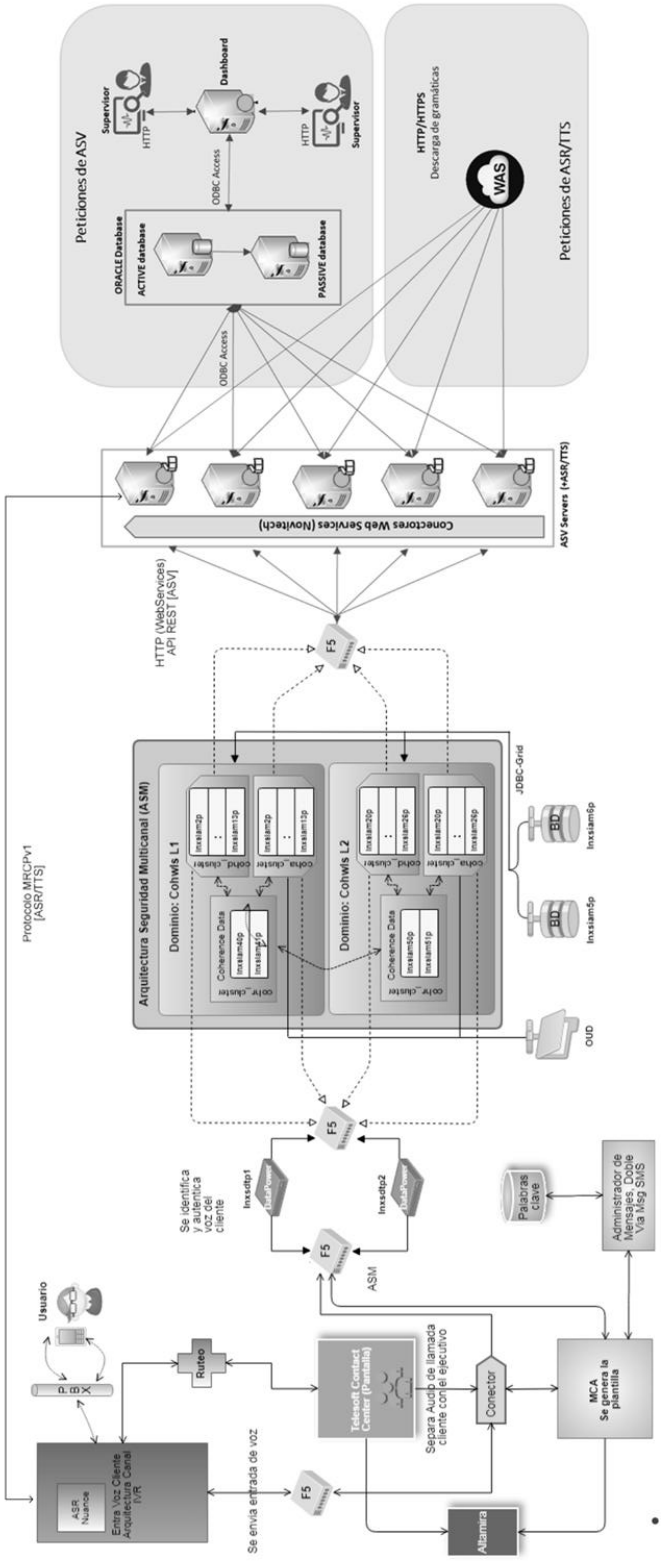

Imagen 10 ARQUITECTURA DE AUTENTICACION POR VOZ A IMPLEMENTAR

METODOLOGÍA UTILIZADA

En el banco, no existe una completa homologación de metodologías, por lo que en este caso se utilizaron Crisol, por parte de TI y SCRUM, design thinking por Innovación.

Después de realizar una pequeña prueba de concepto, definida desde el área de innovación por medio primero del uso del design thinking y posterior a ello por medio de SCRUM, de forma ágil se consiguió hacer una validación de ella por las áreas participantes y en la que se involucró también al usuario. Esta prueba de concepto sirvió para evaluar las diferentes tecnologías que los proveedores nos presentaron. Consiguiendo así una calificación técnica que al conjuntarla con el costo, el área de adquisiciones nos entregó el fallo. (*Imagen 11*).

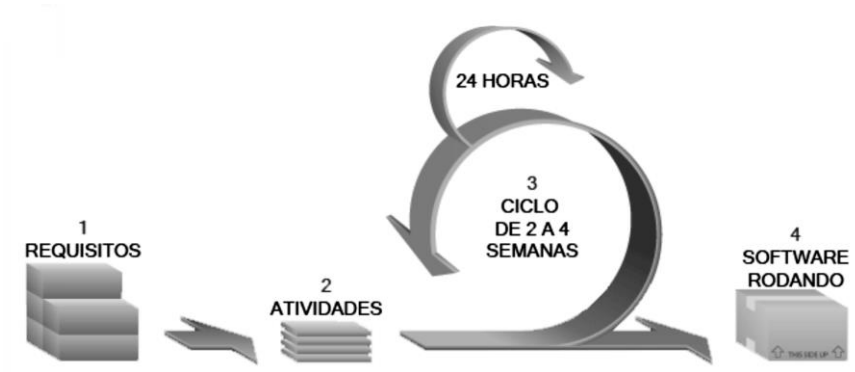

Imagen 11 METODOLOGÍA SCRUM

A partir de esto, se lleva a cabo la solicitud hacia TI y por lo cual entonces, se comienza a utilizar la metodología Crisol. (*Imagen 12*).

Crisol considera dentro de su metodología los siguientes pasos:

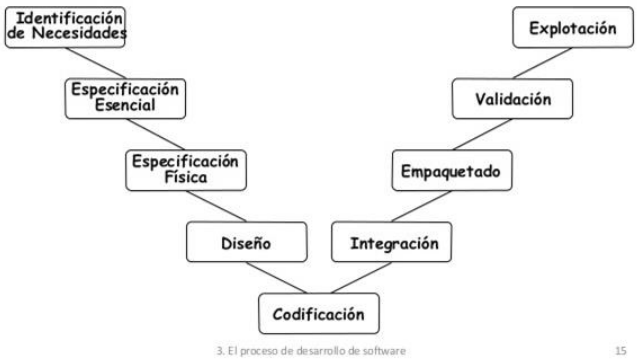

Imagen 12 METODOLOGÍA CRISOL V

El primer paso es identificar las necesidades y documentarlas en su totalidad para conseguir el resultado esperado. Esto con el apoyo del usuario, con base a su experiencia y del área de tecnología e innovación, quienes finalmente buscarán una eficiencia en el proceso y adaptar la herramienta al uso cotidiano.

Después del paso anterior, se definirá la especificación y con la cual se buscará la mejor adaptación del proceso, la herramienta y la arquitectura multicanal. Para ser validados conforme a las necesidades.

El diseño es el cuarto paso en esta metodología y en la cual se buscará definir todos los conceptos requeridos por TI para la interconexión de los componentes. Identificando aquí las necesidades de software y hardware, los equipos de trabajo que participarán y el tiempo que se llevará en el proyecto.

La codificación, como siguiente paso, implica el desarrollo y tropicalización de la herramienta.

Por un lado el proveedor de la aplicación hizo la precalibración a fin de identificar las características de ruido en el entorno del IVR y desde teléfonos móviles y/o fijos, con diferentes acentos desde diferentes participantes femeninos y masculinos y a nivel nacional. Con esta precalibración se obtiene un modelo a considerar dentro de nuestro sistema y con el cual la aplicación convivirá a manera de identificar en las llamadas subsecuentes.

Desarrollo TI por otro lado, codificó lo necesario a fin de conseguir las conexiones de voz entre el IVR y la herramienta. Del mismo modo, lo necesario para conseguir una base de datos con las diferentes características de la llamada: género, estado, número telefónico, etc., por ejemplo.

El siguiente paso, fue la integración entre las diferentes plataformas de la arquitectura multicanal. Adaptación de idioma y protocolos de voz en IVR, base de datos, seguridad multicanal, core bancario, entre otros.

El empaquetado, quedó completamente del lado de tecnología, documentando y definiendo los responsables de desarrollo, seguridad informática e infraestructura. Se siguieron las adecuadas especificaciones del proveedor y cumpliendo las reglas de seguridad informática en cuanto accesos y codificación de llaves.

Para validar, se especificó una matriz de pruebas tanto de ambientes aislados como del total de su implementación. Por un lado con usuarios inexistentes, obteniendo la calibración ideal del ambiente y con todas sus variantes, geográficas, tecnológicas, de genero y lingüísticas. (*Imagen 13*).

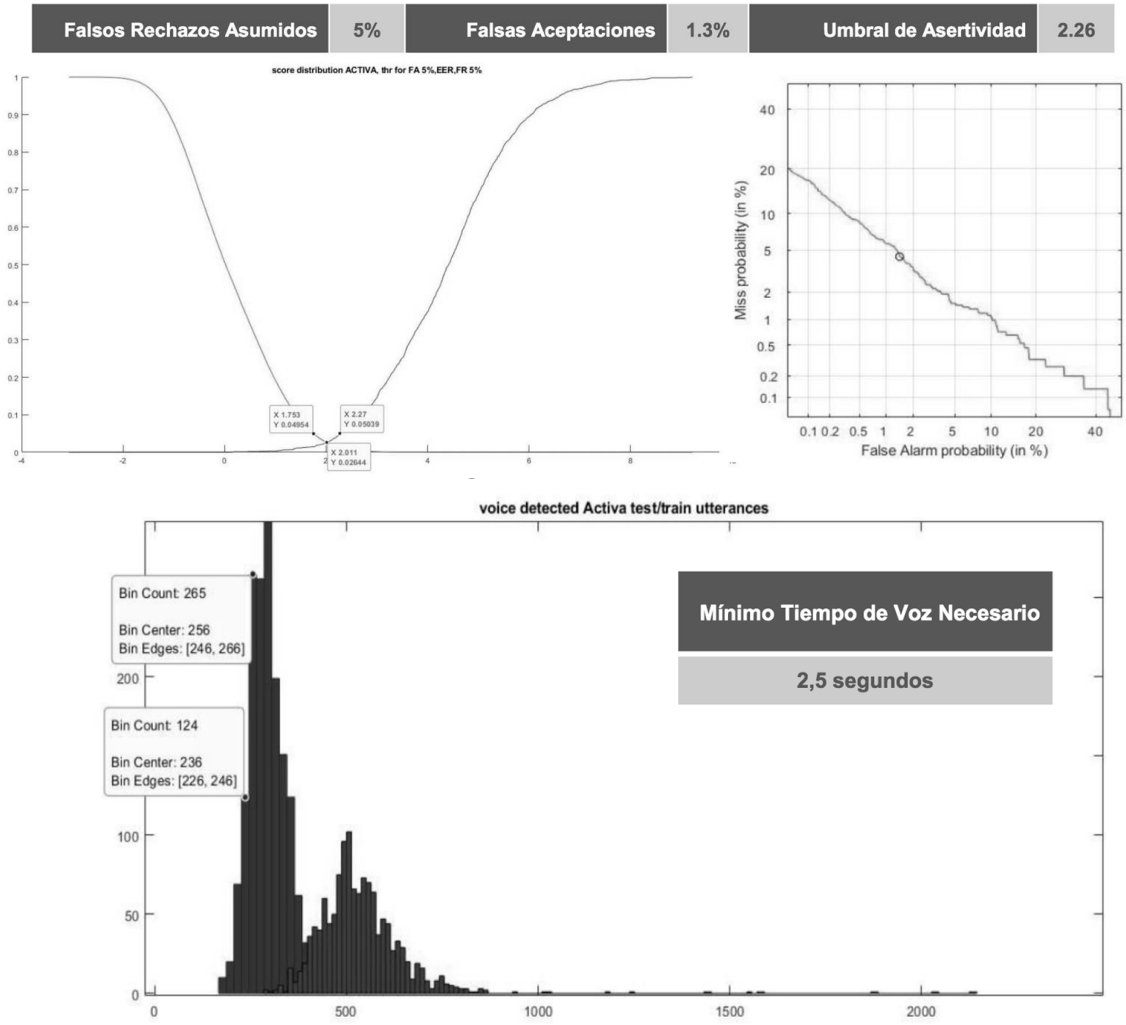

Imagen 13 CALIBRACION DE ESTRATEGIA ACTIVA

Cumpliendo todas las expectativas y corrigiendo los detalles encontrados, se procedió dar el VoBo. a fin de entrar en el paso de explotación. Este paso consideró de inicio, la participación de familiares y amigos internos con cuenta del banco a fin de encontrar detalles dentro de los ambientes productivos, en su caso corregir o agregar puntos en beneficio del cliente y su seguridad.

PARTICIPACIÓN PROFESIONAL

Como líder de Innovación de este proyecto y basado en la experiencia previa durante mi paso por el área de tecnología, mi participación fue basada por un lado en identificar las herramientas con las características requeridas y que prioritariamente no debiesen ser vulnerables por métodos de cualquier tipo, como en este caso, identificar que la voz no fuese suplantada por una grabación. Hecho que en mi caso hizo recurrir a los conocimientos de modulación y demodulación, amplificación de señales y armónicos de las series de Fourier. Desafortunadamente en México es casi nula el diseño de estas tecnologías y por lo cual solo nos queda cuestionar que tipo de tecnologías y algoritmos usan para identificar debilidades, además de las pruebas que lo confirmen. (*Imagen 14*).

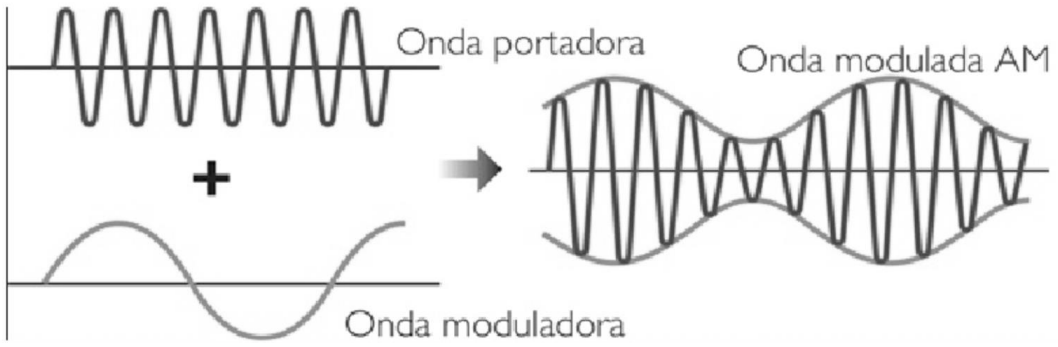

Imagen 14 MODULACIÓN Y DEMODULACIÓN DE VOZ

Conocer la nueva arquitectura multicanal de tecnología, me ayudó bastante en la identificación de la herramienta que cumpliese con los requisitos, además de que durante su implementación y aunado a mis conocimientos de ingeniería, me ayudaron a corregir desviaciones que pudiesen impactar en el resultado y en la parte económica del proyecto.

El seguimiento en las diferentes metodologías fue también participación profesional y en ella, identificar desviaciones, negociar con proveedores, usuarios y diferentes áreas para conseguir que el objetivo se obtenga en tiempo y con las características idóneas para el dueño del canal y principalmente para el usuario final.

La administración de los recursos de las diferentes áreas y del presupuesto necesario, también fue una de mis participaciones. Como responsable, cuantifiqué un presupuesto para conseguir la autorización formal con la dirección del banco, conseguí definir con el área de adquisiciones el proceso de RFI y RFP para seleccionar junto a todos los participantes la mejor herramienta. Gestioné las autorizaciones necesarias con mis superiores para ir liberando los requerimientos de pago a proveedores y fábricas.

Por tratarse de herramientas y procesos innovadores, mi participación fue fungir como intermediario entre los procesos anteriores y los nuevos procesos, definiendo nuevos flujos y pantallas que mejoraran el día a día de la operación diaria. (*Imagen 15*).

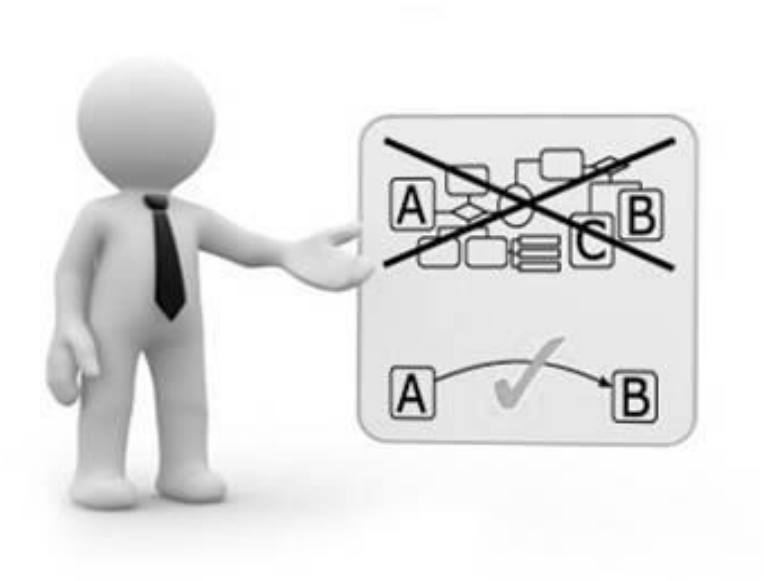

Imagen 15 PROCESOS EFICIENTES

RESULTADOS Y APORTACIONES

Los resultados hasta ahora han sido satisfactorios, el sistema tiene la posibilidad de ir mejorando las huellas vocales, además de que el proceso de enrolamiento de los clientes es paulatino.

Los nuevos procesos generados por la implementación de la herramienta, minimizan la intervención humana conforme a lo esperado y el riesgo disminuye considerablemente, dejando la evaluación de la identidad a una herramienta y no a una encuesta realizada por un humano.

La curva de reducción de costos operativos tiende a la baja y para que la tendencia sea mucho mayor, se requiere que mas de los servicios que se atienden por un humano, se transfieran a este método de autenticación. Esto irá sucediendo conforme se vaya consiguiendo una mayor confianza en la herramienta y junto a la adaptación de nuevos procedimientos.

El sistema genera listas negras y éstas serán usadas para identificar mediante este canal, las huellas vocales que se consideran como defraudadores, haciendo una inmediata identificación y mitigando los futuros riesgos. Esta base de datos se encuentra en un proceso de adaptación a otros sistemas de prevención de fraudes, con esta se busca incrementar la forma de identificar llamadas con este fin.

La autenticación por voz, ahora se buscará adaptar para el uso de otros canales (*Imagen 16*).. Las características de la aplicación nos ayuda a tener una opción más a fin de identificar lo que los usuarios dicen y con esto buscar por un lado la apertura a la banca por voz, en la que por medio de robots se brinde la atención requerida, identificando por medio de lo que el cliente diga, adaptándole a la arquitectura necesaria con el objeto de interconectarlo con la inteligencia artificial y todos los sistemas correspondientes para efectuar la transacción.

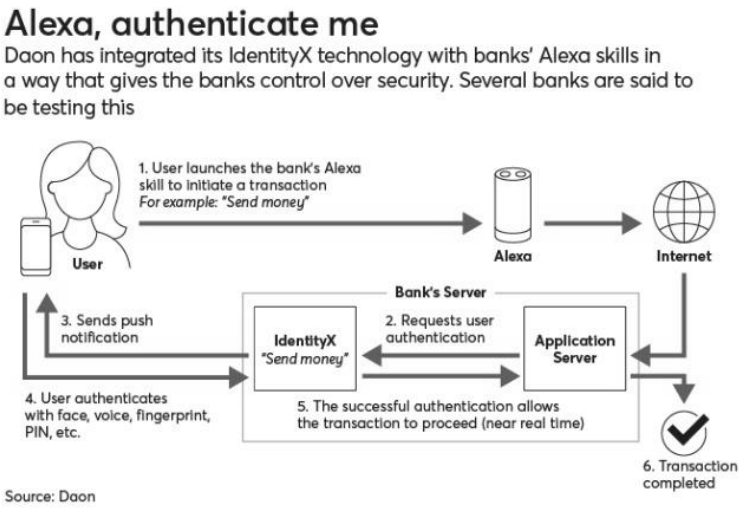

Imagen 16 TRANSACCION EN BANCA POR VOZ

El usuario lanzará su requerimiento por medio de un asistente virtual por voz, viajará el requerimiento por la web y llegará al banco para ser identificado el requerimiento y al ser identificado, se le notificará al usuario la necesidad de hacer una autenticación o no. La autenticación dependerá del tipo de transacción, si es monetaria, requerirá autenticación y si solo es de consulta solo con identificar al usuario se le dará el servicio.

La principal aportación de esta herramienta y dejando atrás lo principal que es la autenticación, se basa principalmente en la identificación de lo que el usuario dice para validar que este diciendo su frase definida como clave o password, esto es:

- Los Chatbots cognitivos utilizan NLU para extraer la intención que hay detrás de una frase y todos los datos adicionales que sean necesarios para poder dar respuesta a dicha intención y aprender activamente de cada conversación.

- Lingüística, data science e inteligencia artificial están involucrados en esta tecnología, la cual evoluciona y mejora su precisión día a día gracias a grandes inversiones en investigación y desarrollo.

La mayoría de los chatbots con los cuales podemos interactuar en las webs o las redes sociales, no incorporan NLU, y la diferencia puede notarse en la naturalidad de la conversación y la precisión en las respuestas a nuestros requerimientos.

CONCLUSIONES

La utilización de mecanismos biométricos de consumo pretende solventar un problema de conveniencia, en detrimento de la seguridad.

Hoy en día todavía hay mucha gente que no configura una contraseña en sus móviles, tabletas u ordenadores por la incomodidad de teclearla cada vez que se utilizan.

Emplear una huella u otros rasgos biométricos para solucionarlo, aunque facilita la usabilidad, no es el modo más adecuado, fomenta que el usuario final no tome conciencia de la importancia de mantener su información segura, y olvide las buenas prácticas en materia de privacidad, como acostumbrarse a memorizar buenas contraseñas, utilizar una para cada servicio, cambiarlas a menudo, o evitar apuntarlas y utilizarlas en lugares donde puedan ser copiadas.

Por todo ello, es recomendable limitar el uso de tecnologías biométricas a aplicaciones donde la seguridad y la privacidad no sean una prioridad, y en caso de serlo, emplearlas únicamente en sistemas de autenticación de doble factor.

Los sistemas de identificación basados en biometría son un bloque importante en el desarrollo de la tecnología, es por esto que industrias líderes consideran que la tecnología biométrica es la más importante tecnología que vamos a ver en los próximos tres años. La biometría es una herramienta que ofrece actualmente el más alto grado de seguridad para la minimización del fraude y la suplantación, en cualquier proceso donde la verificación de identidad sea requerida. Se debe orientar a usuarios hacia la aceptación global de la nueva realidad tecnológica. Las oportunidades para aplicar tecnología biométrica por voz, esta disponible ya como una herramienta.

Las personas de mayor edad olvidan datos como el PIN u otra información personal, lo cual representa un obstáculo cuando quieren ponerse en contacto con la entidad. Por su parte, los clientes más jóvenes también muestran menor paciencia y desean estar cuanto antes en contacto con un agente para hablar con él en lugar de pasar por un sistema automático que les haga varias preguntas para confirmar su identidad.

Al igual que en muchos otros campos, la tecnología sigue avanzando tanto en la mejora de las técnicas utilizadas en los sistemas ya existentes como en el desarrollo de nuevas técnicas. Esto es consecuencia de una demanda cada vez mayor de seguridad en un gran número de campos.

El futuro de los sistemas biométricos se ven reflejados en diferentes aspectos que poco a poco se van consiguiendo:

- Costos Más Bajos.
- Crecimiento de la industria de biométricos.

Hoy en día los sistemas biométricos tienen un lugar importante en una sorprendente variedad de aplicaciones, más allá de controlar el acceso. Inmigración, control de asistencia, asilos, guarderías y centros de atención médica, programas de beneficencia y puntos de venta son solo unas cuantas de las aplicaciones donde se utilizan biométricos y ayudan a hacerlos de mayor uso común.

- Incremento en la Precisión

Se prestó poca atención a dejar entrar a los que estaban autorizados. Para esas aplicaciones, una tasa baja de Falsa Aceptación era el requerimiento más importante.

A medida que estos sistemas se fueron moviendo a aplicaciones comerciales, la Tasa de Falso Rechazo fue tomando importancia.

una Tasa de Falso Rechazo de 1: 100,000 y una Tasa de Falsa Aceptación de 5%.

Las Tasas de Falsa Aceptación requeridas para dispositivos comerciales de control de acceso son severas, pero la necesidad de Tasas de Falso Rechazo también deben ser bajas. Para un uso extendido de biométricos a nivel comercial se requerirán bajas Tasas de Falso Rechazo en sistemas intuitivos y fáciles de usar.

BIBLIOGRAFIA

Book Title

Speaker Authentication

Authors

- Qi (Peter) Li

Series Title

Signals and Communication Technology

Copyright

2012

Publisher

Springer-Verlag Berlin Heidelberg

Copyright Holder

Springer-Verlag Berlin Heidelberg

eBook ISBN

978-3-642-23731-7

DOI

10.1007/978-3-642-23731-7

Hardcover ISBN

978-3-642-23730-0

Softcover ISBN

978-3-642-27088-8

Series ISSN

1860-4862

Book Title

Handbook of Research on Cloud and Fog Computing Infrastructures for Data Science

Authors

- Saleema A.

Series Title

Voice Biometrics: The Promising Future of Authentication in the Internet of Things

Publisher

Indian Institute of Information Technology and Management Kerala, India

SITIOS WEB

Luis Moreno | Jun 10, 2019 | Biometría en el Mundo, La Evolución en los Métodos de pago el uso de rasgos Biométricos

http://biometriaaplicada.com/sitio/la-evolucion-en-los-metodos-de-pago-el-uso-de-rasgos-biometricos-para-brindar-mayor-seguridad-y-comodidad-al-usuario-al-realizar-sus-pagos/

Security and biometrics solutions—Omni-channel customer engagement success stories

https://www.nuance.com/omni-channel-customer-engagement/case-studies/pensiones-banorte.html

Ron Condon |17 Sep 2009 | Strong authentication methods, voice recognition systems make comeback

https://www.computerweekly.com/news/1368621/Strong-authentication-methods-voice-recognition-systems-make-comeback

Gemalto |mar 2019 | Biometría para identificación y autenticación

https://www.gemalto.com/latam/sector-publico/inspiracion/biometria

GLOSARIO

- *IVR* Interactive Response Unit

Es un autómata que responde a una llamada e interactúa con el usuario mediante reconocimiento de voz o tonos. Las locuciones son grabadas previamente o procesadas en tiempo real a partir de un texto.

- *Cola Universal*

La cola única, o en algún entorno llamada cola universal, es una funcionalidad de las soluciones tecnológicas de Contact Center y CRMs que permite que cualquier tipo de interacción se trate por un mismo grupo de atención o cola. Es decir, las llamadas, emails, redes sociales, sms, etc., se encolan en un único grupo, que es donde están asignados los agentes para atender estas interacciones.

- *PBX*

Central telefónica privada. Sistema de conmutación privada, ya sea manual o automática, ubicada en las instalaciones del cliente.

- *MCA* Arquitectura Multi Canal

Arquitectura que interconecta todos los canales de servicio

- *OAM* Oracle Access Manager (OAM)

Oracle Access Manager es una aplicación **J2EE** normalmente implementada en un servidor de aplicaciones Weblogic

- *OID* Oracle Identity Manager (OIM)

El servidor OIM es una aplicación J2EE. El aprovisionamiento de usuarios se realiza en OIM.
El OIM integra esto con todas las otras aplicaciones.

- *ATM* Automated Teller Machine

Máquina conectada informáticamente con un banco que permite efectuar al cliente ciertas operaciones bancarias mediante una tarjeta o libreta magnéticas que tienen asignada una clave personal.

- *SOA* Arquitectura Orientada a Servicios

Marco de trabajo conceptual que permite a las organizaciones unir los objetivos de negocio con la infraestructura de TI integrando los datos y la lógica de negocio de sus sistemas separados.

- *WMBTT* WebSphere Multichannel Bank Transformation Toolkit

Kit de herramienta websphere para transformación multicanal bancario.

- *ABINITIO*

Herramienta que facilita el trabajo de los desarrolladores de aplicaciones, quienes tienen a su cargo el diseño y armado de sistemas sofisticados capaces de procesar grandes cantidades de datos en entornos complejos.