NUANCE

Biometría para empresas de telecomunicaciones

Autenticación de clientes y prevención del fraude.

En colaboración con Microsoft

Índice

Nuance y Microsoft: una colaboración estratégica para prevenir el fraude y mejorar la experiencia del cliente.

Nuance y Microsoft están mejorando la experiencia del cliente y la prevención del fraude en las empresas de telecomunicaciones, agilizando y reforzando la seguridad de los procesos de identificación y verificación de clientes, a través de soluciones de IA y biometría.

Nuance Gatekeeper, incorpora la tecnología de IA y los servicios de confianza de Azure de Microsoft para ayudar a las empresas de telecomunicaciones a:

— **Crear experiencias de mayor calidad para clientes y empleados** gracias a un proceso de autenticación sencillo y seguro.

— **Evitar el fraude y proteger a la empresa** gracias a la detección inteligente y proactiva del fraude.

— **Aumentar los beneficios** al reducir drásticamente los costes operativos y aquellos derivados del fraude.

El servicio en la nube de Microsoft Azure ofrece ventajas de seguridad en una plataforma innovadora de confianza que sustenta a Nuance Gatekeeper. Al combinarse, la solución protege la experiencia de los clientes al identificar a la persona que lleva a cabo cada interacción, lo que permite ofrecer un servicio más personalizado y gestionar y reducir el riesgo de fraude.

En este white paper:

- Conozca cuáles son los factores de riesgo a los que se enfrentan las telcos hoy en día durante la interacción con el cliente
- Descubra cómo funciona la biometría
- Descubra los resultados que están logrando otras empresas de telecomunicaciones

Aunque las redes de telecomunicaciones actuales son muy seguras, el fraude en la industria continúa siendo un reto. Los estafadores, bien sea por su cuenta o a través de redes de crimen organizado, obtienen dispositivos y servicios apoderándose de cuentas con información robada, dan de alta cuentas nuevas con identidades sintéticas y fijan como objetivo a los agentes del servicio de atención al cliente mediante la ingeniería social. Cada fuga de datos de inicios de sesión, contraseñas e información personal pone en manos de los estafadores más y más datos de consumidores.

Resumen ejecutivo

Los resultados del informe Cyber-Telecom Crime 2019, indican que las pérdidas derivadas del fraude en el sector de las telecomunicaciones a nivel global ascendieron a 32.700 millones de dólares[1]. El reporte a las Naciones, edición 2020, que publica todos los años ACFE (Asociación de Examinadores de Fraude Certificados), señala que **las empresas pierden el 5% de sus ingresos debido al fraude cada año.**[2] Si alguien tuviese acceso de forma fraudulenta a la cuenta de un usuario, pudiendo cometer la estafa tanto en una tienda física (haciéndose pasar por el cliente legítimo), en el canal online o a través del *contact center*, podría solicitar una línea adicional en la cuenta, que después podría ser vendida a cambio de dinero en efectivo en la calle. También podría conseguir un teléfono nuevo u otro dispositivo que podría vender inmediatamente a cambio de dinero en efectivo; podría comprar accesorios, una vez más cargando el coste a la cuenta, o podría usar la cuenta de telecomunicaciones del cliente para obtener acceso a información financiera y otras cuentas del cliente.

Los operadores están creando constantemente nuevas formas de interactuar con los clientes que requieran la menor fricción y el menor esfuerzo posibles. Por desgracia, esto favorece al estafador que está alerta esperando descubrir una vulnerabilidad en la infraestructura de atención al cliente del operador. Los ciberdelincuentes –principalmente motivados por intereses económicos – están constantemente innovando y utilizando nuevas técnicas y, en la mayoría de los casos, trabajan en equipo para compartir conocimiento y actividades en tiempo real con el fin de perpetrar un ataque cuando se presente la oportunidad a mayor escala.

iGR, una consultora de análisis de mercado especializada en la industria de las comunicaciones móviles e inalámbricas, ha llevado a cabo numerosas investigaciones en los últimos años sobre cómo los clientes interactúan con los operadores: de media, según iGR, cada cliente llama al servicio de atención al cliente una vez por trimestre, a través de todos los canales y en relación con la población en general. Pero no todo el mundo llama cada mes; de media, los usuarios que se ponen en contacto con el servicio de atención al cliente lo hacen cada dos meses.

17%

de los clientes que cambiaron recientemente de operador móvil afirmaron que el motivo del cambio fue el servicio de atención al cliente o un problema relacionado con la facturación.

1876
millones

de interacciones con clientes necesitan autenticarse (y para 2025, GSMA prevé que el número total de interacciones llegará a los 2000 millones)

Y no es ninguna sorpresa que la calidad del servicio de atención al cliente de un operador móvil es un factor determinante de la tasa de abandono. Según una reciente encuesta de iGR, casi el 17% de los clientes que habían cambiado recientemente de operador, afirmaban que el motivo del cambio fue el servicio de atención al cliente o un problema relacionado con la facturación.

En la actualidad, el número de clientes móviles en Europa supera los 469 millones.[3] Si el cliente medio se pone en contacto con el operador para recibir asistencia cuatro veces al año, se producen 1876 millones de interacciones de atención al cliente. Esto significa que 1876 millones de interacciones deben autenticarse. Y para 2025, GSMA prevé que el número total de interacciones llegará casi a los 2000 millones.

Cada una de estas interacciones requiere algún nivel de autenticación, y cada autenticación es una oportunidad para que la experiencia del cliente sea buena o mala. Es más, cada una de estas interacciones podría ser un intento de un estafador por hacerse con la cuenta de un cliente. Las telcos, por tanto, deben encontrar la manera de proteger a sus clientes sin añadir fricción y frustración innecesarias a sus experiencias.

Como podrá leer a lo largo de este white paper, la mayoría de las telcos más importantes del mundo están adoptando la biometría para lograr una autenticación fluida que mejore la experiencia del cliente y evite el fraude de forma proactiva para proteger las interacciones.

Hoy en día, las telcos se enfrentan a problemas fundamentales que son un desafío para su actividad principal:

1. Proteger a clientes y suscriptores.
2. Verificar la identidad de los clientes de forma fiable sin añadir fricción innecesaria.
3. Reducir los costes de los agentes y el tiempo de gestión de la llamada.
4. Ofrecer una experiencia coherente y personalizada en todos los canales.

La biometría se está adoptando por muchos motivos:

— La biometría **abarca todos los canales de interacción con el cliente** que puede ofrecer un operador, desde el canal telefónico / voz (agentes físicos y sistemas de respuesta de voz interactivos) hasta lo digital (web, apps móviles y apps de mensajería).

— La autenticación biométrica ha demostrado mejorar **la experiencia del cliente,** aumentar la productividad del agente y reducir el tiempo medio de gestión de la operación con el cliente, al mismo tiempo.

— Además de mejorar la autenticación de los clientes legítimos, la biometría **detecta y evita el fraude de manera simultánea.**

Problemas de los riesgos actuales

Cualquier persona que se haya puesto en contacto con su operador móvil sabe lo que hay que hacer: llamar o iniciar sesión y, después, contestar a una serie de preguntas para confirmar la identidad. En la web, por ejemplo, el método habitual es solicitar un inicio de sesión y contraseña y, después, antes de poder hacer una compra, confirmar la identidad del titular de la cuenta con una pregunta de seguridad o autenticación de doble factor, como el envío de un enlace por correo electrónico o un código PIN por SMS.

Hoy en día, las redes LTE son muy seguras y pueden detectar dispositivos no autorizados en la red. Pero sigue siendo posible obtener de forma fraudulenta dispositivos y servicios a través de los canales de atención al cliente cuando alguien se intenta hacer pasar por el cliente real. Cada fuga de datos de inicios de sesión, contraseñas e información personal agrava el problema.

Si alguien puede acceder de forma fraudulenta a la cuenta del cliente, bien sea en una tienda, online o a través del *contact center*, esta persona podrá:

— Solicitar una línea extra en la cuenta, que después se podrá vender por dinero en efectivo en la calle y que para cuando el cliente y el operador descubran el fraude, el teléfono o la SIM ya se habrán vendido.

— Obtener un nuevo teléfono u otro dispositivo (que se cargará a la cuenta) y que, una vez más, podrá venderse a cambio de dinero.

— Obtener accesorios que, una vez más, se cargarán a la cuenta.

— Usar el acceso a la cuenta de telecomunicaciones para obtener cualquier tipo de información o acceso a otras cuentas, como cuentas bancarias, etc.

Obviamente, los operadores móviles emprenden acciones para verificar la identidad de los clientes verdaderos. Pero a medida que toman más precauciones, la interacción con el cliente se hace más invasiva y molesta. Por ejemplo, la experiencia del autor de este white paper con un importante operador móvil requirió la autenticación de su identidad tres veces, de tres formas distintas. Durante la llamada inicial se autenticó con la típica pregunta de seguridad basada en el conocimiento (KBA) antes de pasar a otro departamento para solucionar el problema. La segunda interacción requirió otra nueva pregunta de seguridad. Finalmente, la llamada se derivó al servicio de asistencia técnica, que volvió a verificar la identidad del cliente, esta vez, mediante el envío de un código PIN. Hay que tener en cuenta que, en muchos casos, el estafador tiene información personal del cliente en su poder, y que el titular de la cuenta real puede olvidar su PIN o contraseña.

El problema con los métodos de autenticación actuales es que, además de estar demostrado que hace años que dejaron de ser seguros, son muy molestos para el cliente. Recordar todas las respuestas que seleccionamos en las preguntas de seguridad, las innumerables e indescifrables contraseñas que nos obligan incluso hasta cambiar cada cierto tiempo y otros datos, dificulta la operativa y puede sobrecargar la interacción con el operador móvil. Esto aumenta la fricción entre los clientes y el operador y el nivel de esfuerzo necesario por parte del cliente. Muchos consumidores recurren a escribir las respuestas en un papel o a usar preguntas y respuestas sencillas y fáciles de recordar y de averiguar. Un hecho que facilita el trabajo al estafador.

En resumen, las telcos deben resolver dos problemas básicos de primera necesidad: (i) cómo autenticar fácilmente al cliente y con la menor fricción posible cuando este contacta con el servicio de atención al cliente y/o accede al área de cliente; y cómo evitar el fraude en todos los canales de atención al cliente.

Las telcos deben resolver dos problemas básicos:

1. Cómo autenticar fácilmente a los clientes, con la menor fricción posible, cuando contactan con el servicio de atención al cliente y/o acceden al área de cliente.
2. Cómo evitar el fraude en todos los canales que el cliente utiliza para comunicarse con la empresa.

La magnitud del problema

Según el informe Cyber-Telecom Crime 2019, las pérdidas por fraude a nivel global fueron de 32.700 millones de dólares. Obviamente, si los operadores móviles divulgan una posible debilidad, es más probable que los estafadores traten de aprovechar esa debilidad.

Determinar la magnitud del problema, pasa por comprender la magnitud de la operativa de atención al cliente en la industria de las telecomunicaciones. La consultora especialista en telecomunicaciones iGR, ha llevado a cabo numerosas investigaciones en los últimos años sobre cómo los clientes interactúan con los operadores:

— De media, según iGR, cada suscriptor llama al servicio de atención al cliente una vez por trimestre.

— No todos llaman cada mes. Lo normal es que los clientes intenten resolver el mismo problema varias veces desde distintos canales.

— Según las investigaciones de iGR, el 35% de los clientes no ha contactado con el servicio de atención al cliente durante el último año, y el 15% lo ha hecho solo una vez.

— Los clientes que se ponen en contacto con el servicio de atención al cliente lo hacen, de media, cada dos meses.

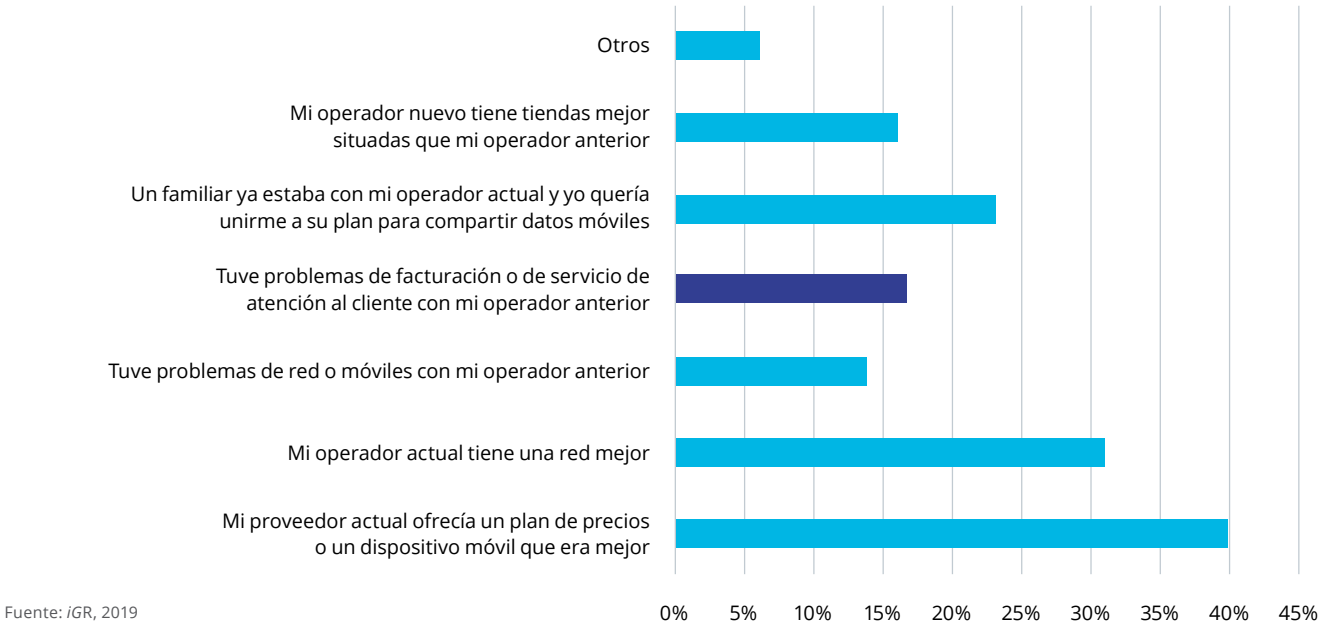
32.700 millones de dólares

en pérdidas por fraude a nivel global en 2019[4]

Por qué es importante la atención al cliente

Todos sabemos que la calidad del servicio de atención al cliente es un factor que determina la tasa de abandono. Como muestra la figura 1, cerca del 17% de los clientes que cambiaron recientemente de operador afirmaron que el motivo del cambio fue el servicio de atención al cliente o un problema con relacionado con la facturación.

Figura 1: motivos para cambiar de operador móvil



Fuente: *iGR*, 2019

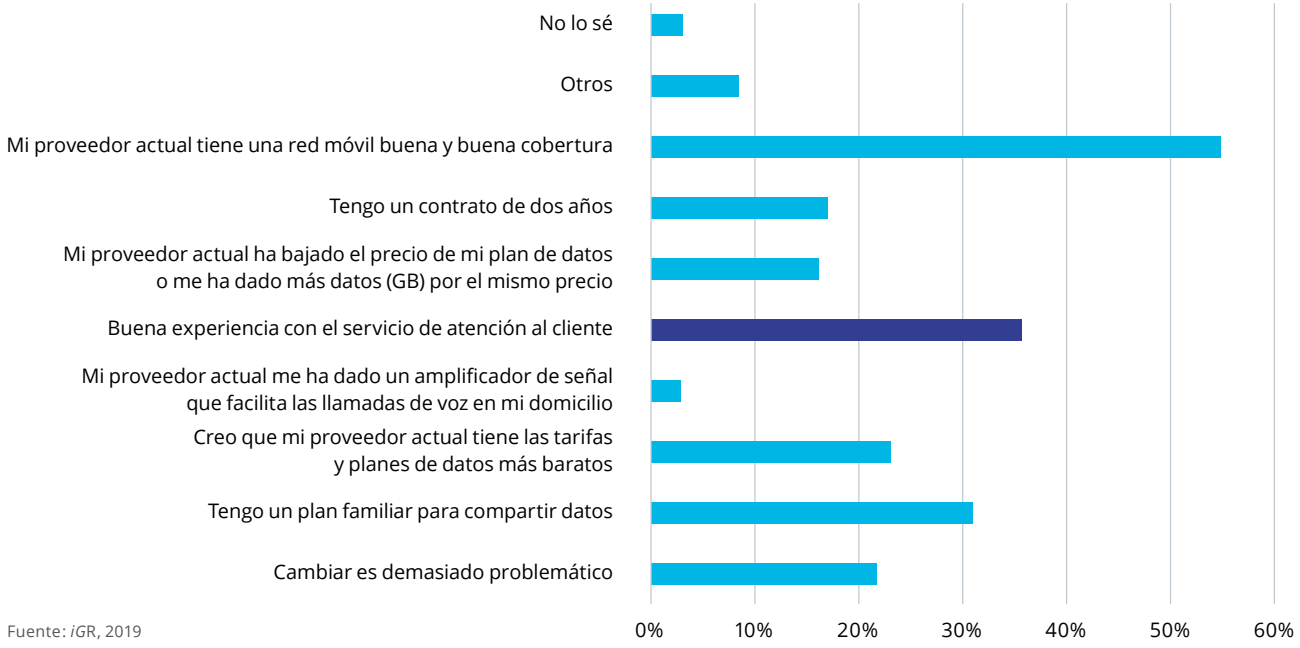
motivo para no cambiar y quedarse con el operador móvil actual. La figura 2 muestra los motivos por los que los clientes eligen quedarse con su operador móvil actual. En este caso «la buena atención al cliente» es el segundo motivo más popular, después de la calidad de la red.

Así, la calidad del servicio de atención al cliente que ofrece un operador móvil es fundamental para fidelizar clientes y evitar el abandono. Hay que tener en cuenta que la tasa de abandono le sale caro al operador: según el análisis de iGR, el coste medio de adquisición de un cliente de un operador móvil en US es de 362 dólares. Por lo tanto, es **mucho más barato retener a un cliente existente** que sustituir a un cliente perdido.

Para que la atención al cliente sea satisfactoria, la autenticación debe ser lo más fluida y lo menos molesta posible. Los procesos de autenticación largos añaden fricción y frustración a la experiencia del cliente, lo que puede hacer que cambien de operador.

Además, los clientes esperan no tener que volver a identificarse al cambiar de canal, pero estas expectativas no se cumplen. Según Gladly, el 71%[5] de los consumidores dice que desea una experiencia consistente en todos los canales, pero solo el 29% afirma conseguirla. Asimismo, según un informe de Microsoft, el 72%[6] de los consumidores espera que sus empresas les reconozcan y sepan quiénes son, qué han comprado y cuándo fue la última vez que se pusieron en contacto con la empresa.

Figura 2: Motivos para quedarse con el proveedor de servicios de telefonía móvil actual



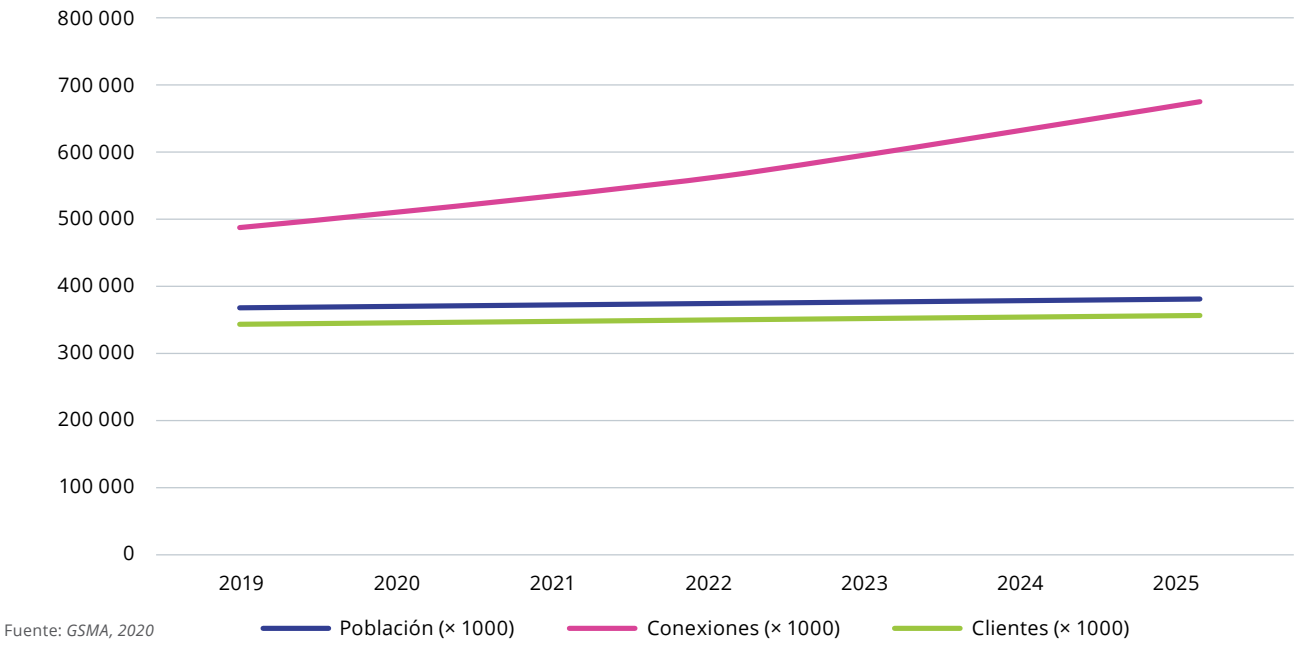
Fuente: *iGR*, 2019

La necesidad de una autenticación fluida y segura es cada vez más urgente ahora que los usuarios recurren al móvil en primer lugar. Como puede verse en la figura 3, aunque el número de clientes móviles aumenta muy lentamente (ya que la mayoría de las personas ya tiene un dispositivo móvil), el número de conexiones móviles que se llevan a cabo está creciendo con rapidez debido al mayor uso de tabletas, TV inteligentes y dispositivos Smart Home, además de otros dispositivos conectados. Cada una de estas interacciones requiere algún nivel de autenticación, y cada autenticación es una oportunidad para que la experiencia del cliente sea buena o mala.

Los operadores móviles también se enfrentan al reto de reducir los costes operativos, incluidos los del servicio de atención al cliente. Según las estimaciones de iGR, a una telco le cuesta aproximadamente un dólar por minuto atender al cliente en todos los canales. (Incluido el tiempo que el cliente está esperando «en cola»). Así que, cuanto más dure la interacción con el cliente, incluido el tiempo para identificarle y verificar su identidad, más cara será la llamada. Y, a medida que aumenta el número de interacciones en el servicio de atención al cliente, el coste por interacción debe reducirse lo máximo posible.

Asimismo, cada vez está menos clara la distinción entre el operador móvil tradicional y el Operador de Múltiples Sistemas (MSO), ya que ambos ofrecen servicios de telefonía móvil, internet y TV. La necesidad de ofrecer una experiencia positiva al cliente es ahora más importante que nunca, ya que el valor de un solo cliente en todos los canales ha aumentado de manera considerable.

Figura 3: población de Europa, conexiones móviles y clientes móviles (2019-2025) (× 1000)



Fuente: *GSMA, 2020*

Para poner esto en perspectiva, hagamos unos cálculos básicos:

— A finales de 2019, había menos de 469 millones de clientes móviles en Europa y 675 millones de conexiones móviles. Si el cliente medio se pone en contacto con el operador por motivos de asistencia cuatro veces al año, esto se traduce en 1876 millones de interacciones de atención al cliente. Esto significa que 1876 millones de interacciones deben autenticarse.

— Para 2025, GSMA prevé que habrá 480 millones de clientes, pero casi 679 millones de conexiones. Si cada suscriptor se pone en contacto con su operador móvil cinco veces al año (un aumento debido al mayor número de dispositivos), el número total de interacciones será de 2400 millones. Esta cifra es bastante conservadora, dado el aumento considerable del número de conexiones.

Los proveedores de servicios de comunicaciones necesitan una manera de mejorar la experiencia del cliente sin poner en peligro la seguridad. Deben aumentar la seguridad activa para proteger a sus clientes sin añadir fricción y frustración innecesarias. Aquí es donde entran en juego las soluciones de autenticación y prevención del fraude.

Cómo funciona la biometría

La biometría es el nuevo estándar para autenticar clientes y prevenir el fraude en las empresas de telecomunicaciones, instituciones financieras, empresas del sector público y otras industrias. Los consumidores interactúan con regularidad con los sistemas biométricos, bien sea de forma activa o pasiva:

— **Soluciones basadas en dispositivos que usan la biometría facial o las huellas dactilares para acceder al dispositivo móvil.** Estos factores son populares para iniciar sesiones de usuario o acceder a las aplicaciones móviles, pero no ofrecen la seguridad suficiente en las interacciones de mayor riesgo y están limitadas al dispositivo del usuario, lo que hace que no puedan usarse en el *contact center*.

— **Biometría de voz en los sistemas de respuesta de voz interactiva (IVR) y con agentes físicos de atención al cliente.** Las soluciones de biometría de voz verifican la identidad de los clientes legítimos e identifican a los estafadores comparando el audio de la voz entrante con una base de datos de huellas de voces almacenadas, tanto de clientes legítimos como de estafadores recurrentes reconocidos. La autenticación por voz puede completarse durante los primeros segundos de la conversación del cliente con un agente físico o con una IVR conversacional. La biometría de voz se está incorporando cada vez más en las aplicaciones móviles y web, ya que es la forma más rápida y segura de realizar la autenticación de doble factor requerida por el reglamento SCA (Strong Customer Authentication) de la PSD2 (Directiva Europea de Pagos).

— **La biometría del comportamiento, funciona en un segundo plano durante la sesión** del usuario digital para autenticar y detectar el fraude basándose en cómo interactúa una persona con su dispositivo. Entre otros factores, esta modalidad biométrica analiza la velocidad a la que escribe el usuario, el tiempo que mantiene pulsadas las teclas, las pausas que hace, cómo usa el ratón o se desliza por la pantalla. La biometría conductual o biometría del comportamiento, es un factor ideal para la autenticación continua y la supervisión del fraude en aplicaciones móviles y entornos web.

— **La biometría conversacional en aplicaciones de envío de mensajes y entornos con agentes físicos,** analiza el texto escrito y su transcripción para autenticar y detectar el fraude analizando la elección de las palabras que escribe o dice el usuario, la gramática y la estructura de las frases, el uso de emojis, acrónimos y otros elementos. De esta forma, la biometría conversacional añade una capa de autenticación adicional que detecta otros patrones de fraude, como por ejemplo los scripts (guiones) que utilizan y están obligados a leer las personas contratadas para cometer este tipo de fraude, conocidas como «mulas».

CASO DE ÉXITO

Deutsche Telekom

Deutsche Telekom es uno de los operadores de telecomunicaciones más importantes del mundo, con 168 millones de suscriptores móviles, 28 millones de abonados a la red de telefonía fija y 19 millones de líneas de banda ancha en varios países.

La compañía se enfrentó al reto de ofrecer a sus clientes una forma segura, pero cómoda, de acceder a sus cuentas. Su solución consistió en implementar la autenticación por voz de Nuance, lo que eliminó la necesidad de que los suscriptores tuvieran que recordar su número de cliente de 10 dígitos.

El resultado es una autenticación rápida y fluida que permite a los agentes centrarse en las necesidades de los clientes y poder ofrecerles servicios adicionales. Más de 200 000 clientes registraron su huella de voz durante los primeros cinco meses.

75%

de los clientes opina que la autenticación por voz es mucho más cómoda

La evolución de la biometría en las telecomunicaciones

Las telcos de hoy en día se enfrentan a cuatro problemas fundamentales cuando se trata de autenticar al cliente:

1. Verificar de forma fiable la identidad de cada cliente sin fricción innecesaria y sin comprometer la seguridad.
2. Proteger a los clientes de la suplantación de identidad, SIM Swapping, la apropiación indebida cuentas, y otros tipos de fraude.
3. Reducir los costes operacionales y aumentar la eficiencia de los agentes.
4. Ofrecer una experiencia consistente y personalizada en todos los canales.

Las formas de autenticación tradicionales debilitan los esfuerzos de las telcos para afrontar estos retos. Los PIN, contraseñas y las preguntas de seguridad dependen de la memoria del cliente y añaden más fricción y frustración a su experiencia. Los agentes no hacen más que interrogar a los clientes en lugar de ayudarlos, y una mala experiencia puede acabar en una pérdida del cliente. Además, estos factores son sumamente vulnerables para los estafadores que pueden conseguir fácilmente la información del cliente a través de técnicas de ingeniería social, ataques de phishing, las redes sociales, los propios agentes del *contact center*, o comprando la información en las darkwebs.

Para reducir la fricción en este proceso, las telcos han comenzado a utilizar la biometría en los procesos de autenticación. Los primeros factores biométricos que implementaron las telcos fueron las huellas dactilares y el reconocimiento facial. Una vez que los consumidores se acostumbraron a ellos porque venían incorporados en los dispositivos móviles de Apple, Samsung y otros fabricantes, estos factores crecieron en popularidad. Face ID y los lectores de huellas dactilares se convirtieron rápidamente en la norma para iniciar sesión en los dispositivos móviles y aplicaciones, y para autenticar las transacciones pequeñas de bajo riesgo.

Sin embargo, como hemos dicho antes en este white paper, estos factores biométricos que dependen del dispositivo tienen desventajas inherentes que limitan su aplicabilidad. Por ello, las telcos están recurriendo a otras modalidades biométricas para autenticar a los clientes y prevenir el fraude, como la biometría de voz, de comportamiento y la biometría conversacional.

Hoy en día, las telcos pueden hacer uso de las soluciones biométricas basadas en algoritmos de IA de última generación, con detectores del entorno y herramientas contra la suplantación de identidad (anti-spoofing) que verifican la identidad de los clientes legítimos de forma rápida y segura y son capaces de detectar a posibles estafadores. Las mejores soluciones de este tipo pueden integrarse en los canales de voz y digitales para agilizar y proteger cada interacción del cliente, independientemente del canal utilizado.

CASO DE ÉXITO

Telefónica

Telefónica, compañía líder del sector de las telecomunicaciones, con más de 344 millones de clientes en 14 países por todo el mundo, actuó rápidamente durante los primeros días de la pandemia para priorizar las llamadas de las personas mayores de 65 años, mediante la implementación de tecnología de biometría de voz e IA.

El proyecto se llevó a cabo en tan solo 2 semanas y permitió al segmento más vulnerable de la población, recibir atención inmediata y personalizada por teléfono, mientras derivaban otras consultas a otros canales evitando el colapso en el servicio de atención al cliente y mejorando, notablemente la experiencia de sus clientes y la operabilidad del Contac Center.

Los resultados inmediatos fueron impresionantes, con una tasa de éxito del reconocimiento del 97% y una reducción del 60% de las llamadas de clientes menores de 65 años atendidas por los agentes del call center.

Durante los primeros 4 meses del despliegue, Telefónica consiguió procesar más de 25 millones de llamadas, priorizando y protegiendo con éxito a este segmento de clientes.

97%

de éxito en el reconocimiento

La biometría funciona mejor cuando se combina con otras tecnologías de autenticación y detección del fraude, incluidos los detectores del entorno y las herramientas anti-spoofing contra la suplantación de identidad, como:

— La huella del dispositivo para determinar si el dispositivo utilizado por el usuario coincide con el tipo de dispositivo que usó el usuario anterior, sea cual sea el canal.

— Identificación de la red para evaluar el riesgo de una llamada basada en la pérdida de información en el canal de comunicaciones.

— Identificación del país, región o ciudad a la que se asocia una llamada o sesión de usuario para detectar cambios de ubicación sospechosos.

— Validación de la llamada para detectar ANI (Identificación Automática de Números) falsas y rutas de llamadas sospechosas.

— Voces sintéticas y detección de grabaciones para detener a los estafadores que utilizan técnicas de imitación para copiar a los usuarios legítimos.

Las soluciones de autenticación y prevención de fraude modernas, como las que ofrece Nuance, combinan todos estos elementos en un motor de riesgos de IA centralizado. Este método multifactor por capas crea una visión de alta fiabilidad de la persona que utiliza el dispositivo o que está al otro lado del teléfono. Esto, a su vez, logra un mayor grado de éxito de autenticación y una mayor detección del fraude, y permite una personalización detallada al identificar al cliente real que participa en cada interacción.

Según los estudios de Financial Fraud Action UK, la biometría de voz puede ayudar a reducir el coste del fraude en un *contact center* un 90% y en el canal móvil, un 80%. Asimismo, un importante operador móvil de US ha desarticulado redes de fraude organizado gracias a una solución de Nuance, evitando más de 4000 intentos de fraude confirmados y ahorrando una media de 2000 dólares por caso, lo que se traduce en una reducción de las pérdidas por fraude de entre 1 y 3 millones de dólares al año.

90 % de reducción en el coste del fraude en el *contact center* gracias a la biometría de voz

Además de reducir el riesgo potencial del fraude y la apropiación indebida de cuentas, la biometría también puede reducir la tasa de abandono. El 82% de los consumidores se han ido de una compañía debido al mal servicio de atención al cliente, según Zendesk, y como hemos dicho antes, los problemas del servicio de atención al cliente son los que más provocan que los usuarios cambien de operador móvil.

Al reducir el fraude, la fricción y el esfuerzo de los clientes y agentes, tanto el operador móvil como el operador de servicios múltiple (MSO) y los consumidores salen ganando.

La biometría ayuda a las telcos a reducir la tasa de abandono y aumentan el valor del ciclo de vida del cliente al reducir la fricción en las interacciones con el servicio de atención al cliente, además de permitir a los agentes prestar un servicio eficiente y personalizado.[7]

94% de los agentes de un cliente de Nuance señala que la autenticación por voz facilita la prestación de un servicio de calidad.

MÁS INFORMACIÓN

- ☐ Descubra cómo Nuance Gatekeeper ofrece una autenticación biométrica fácil y segura para mejorar la eficiencia operativa de su departamento de atención al cliente y prevenir el fraude de manera proactiva.
- ☐ Escuche la historia real de una víctima de fraude a la que suplantaron su identidad para duplicar la tarjeta SIM de su teléfono y vaciaron sus cuentas bancarias en menos de 24 horas.
- ☐ Descubra cómo la biometría de Nuance permite a Telefónica priorizar y proteger a las personas mayores en su servicio de atención al cliente a través de la voz.

NOTAS A PIE DE PÁGINA:

1 Cyber-Telecom Crime Report 2019
2 Informe a las Naciones de la ACFE 2020
3 https://www.statista.com/statistics/794204/unique-mobile-subscribers-europe/
4 GSMA, The Mobile Economy Report 2020
5 Cyber-Telecom Crime Report 2019
6 Aunque el 71 % de los consumidores dice que desea una experiencia coherente en los distintos canales, solo el 29 % afirma conseguirla. (Gladly, informe sobre las expectativas del cliente)
7 El 72 % de los consumidores espera que los agentes ya sepan quiénes son, qué han comprado y cuándo fue la última vez que se pusieron en contacto con la compañía («2017 State of Global Customer Service Report», Microsoft)
8 https://www.zendesk.com/resources/why-companies-should-invest-in-the-customer-experience/

Sobre Nuance Communications, Inc.
Nuance Communications (Nuance) es pionera y líder en innovaciones de IA conversacional biometría. El 85% de las empresas Fortune 100 de todo el mundo y el 77% de los hospitales de US confían en nosotros. Nuance crea soluciones intuitivas que aumentan la capacidad de las personas para ayudar a los demás.