NUANCE

Las razones principales por las que un proceso engorroso de identificación y verificación puede perjudicar su negocio.

Recomendaciones para empresas que necesitan reducir la fricción y aumentar la seguridad al mismo tiempo.

eBook
Replantear los procesos
de Autenticación de Clientes

¿Le quita el sueño la autenticación del cliente?

No es el único.

Si es responsable de la experiencia del cliente o su función está relacionada con los procesos de autenticación de clientes en su organización, es posible que su trabajo le haya generado alguna que otra noche de insomnio.

El proceso de verificación de clientes de una institución financiera es fundamental para garantizar que los clientes perciben una buena experiencia sobre su marca. Y si no lo es, lo más probable es que sus clientes se vayan a la competencia.

La realidad es que no es la única persona a la que le preocupa. Los procesos tradicionales de autenticación basados en tokens y otros elementos de posesión y conocimiento pueden comprometer la experiencia del cliente y producir grandes quebraderos de cabeza en el contact center de su empresa y a los responsables de prevención del fraude.

En este documento exploraremos cómo muchos de sus problemas se pueden resolver y para ello, nos remontaremos a los orígenes.

También explicaremos por qué merece la pena reunir a todas las partes implicadas para rediseñar su estrategia de identificación y verificación de clientes, y hablaremos de los beneficios que todos ellos pueden recibir a cambio de evolucionar los procesos de autenticación, apostando por un modelo más sencillo y seguro, incorporando la tecnología de IA y biometría de voz.

El **96 %**

de los clientes pierde la confianza y el interés en una empresa después de haber experimentado un proceso demasiado largo y complicado en sus interacciones.

Gartner[1]

1 Gartner, a través de su informe I&D de identificación, biometría al rescate.

La pirámide del dolor de la autenticación

Cada vez que un cliente olvida su contraseña o es víctima de una estafa, su angustia provoca un efecto dominó que se extiende por toda su empresa.

El 77 %

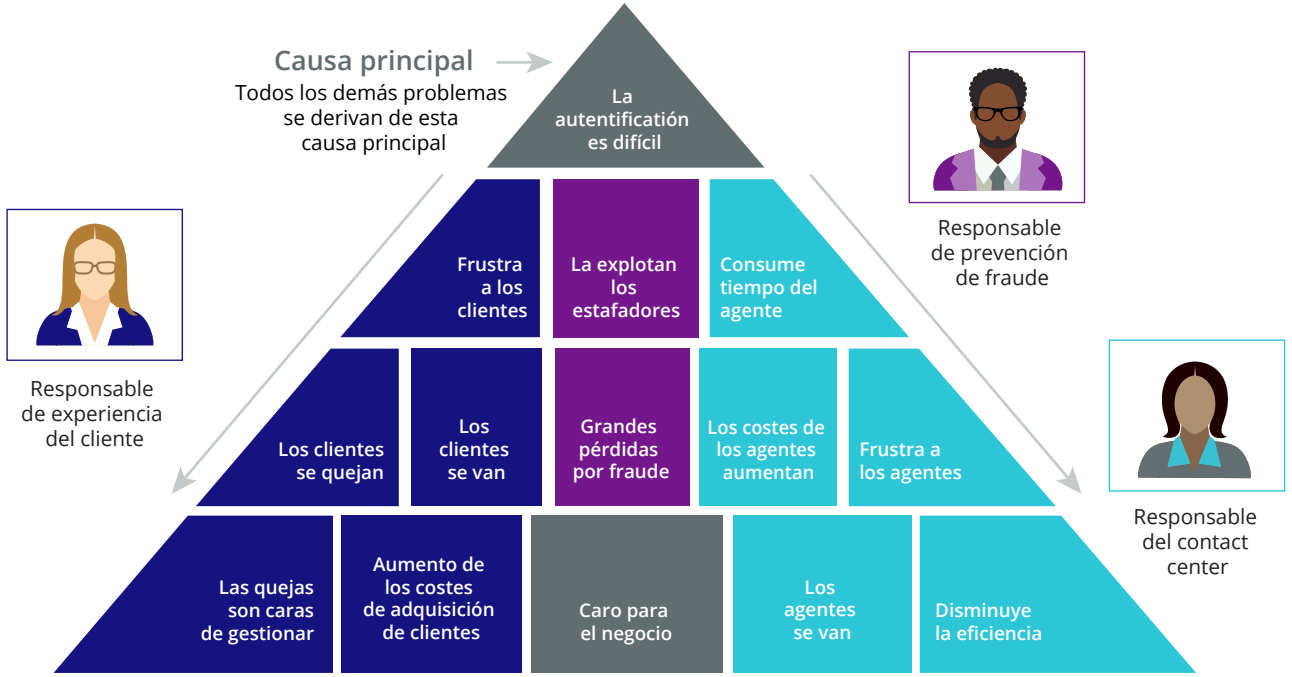
de los clientes quieran cambiar de proveedor de servicios.[2]

La angustia que *usted* siente

Las experiencias de autenticación lentas y difíciles frustran a sus clientes. Generan quejas, que a menudo son transmitidas públicamente a través de las redes sociales, y su organización debe dedicar tiempo y recursos para responder con la debida sensibilidad y rapidez.

Pero aún más, la frustración de un cliente puede hacer que abandone su empresa para siempre. PwC informa que una sola interacción frustrante con un agente es suficiente para que el 77% de los clientes quieran cambiar de proveedor de servicios.[2]

Para empeorar las cosas, es más difícil ganar nuevos clientes cuando otras marcas pueden atraerlos con experiencias de autenticación más sencillas, basadas en tecnologías más modernas. La competencia en este área es cada vez más feroz, y el 96% de las empresas ahora ven la verificación de la identidad como un valor diferencial.[3]



2 PwC, encuesta de 2017 "La experiencia lo es todo", investigación completada en 2018.
3 Séptimo Informe anual sobre fraude de IDology, octubre de 2019.

La angustia que sienten los responsables de prevención del fraude

La angustia de trabajar con procesos de autenticación desfasados y tradicionales la siente con la misma intensidad su equipo de prevención de fraude.

La autenticación basada en elementos de conocimiento, fuerza a sus agentes a trabajar como si fuesen porteros de seguridad. Incluso un agente con mucha experiencia puede ser víctima de ingeniería social. Lo que permite al delincuente acceder a la cuenta de un cliente o a información personal que se puede utilizar en ataques posteriores.

Pero muchos delincuentes no necesitarán engañar a sus agentes para que revelen información confidencial. Ya la habrán comprado en la dark web.

Incluso si no tienen la contraseña de un cliente, existe la posibilidad de que puedan descifrarla. En un análisis reciente de más de mil millones de credenciales filtradas, se incluían 168.919.919 contraseñas, y se descubrió que el 42% eran vulnerables a ataques rápidos de diccionario. Y una de cada 142 contraseñas era "123456".[4]

15
mil millones

de combinaciones de nombre de usuario y contraseña de cuentas están a la venta en Internet, incluidas las cuentas bancarias.[5]

La autenticación basada en tokens, por ejemplo, al enviar un código al teléfono de un cliente, también tiene sus problemas. Un estafador con acceso a la cuenta móvil de su cliente solo tiene que cambiar su número a otra SIM antes de hacer el ataque.

La conclusión es la siguiente: las tecnologías tradicionales de autenticación de clientes son demasiado vulnerables, lo que genera altos costes de prevención del fraude y elevadas pérdidas por fraude.

4 Estudio Digital Shadows notificado a través de ZDNet, julio de 2020.
5 ZDNet informa sobre un análisis de más de mil millones de credenciales filtradas que incluían 168 919 919 contraseñas, julio de 2020.

La angustia que sienten los responsables del contact center

Hacer preguntas de autenticación basadas en el conocimiento lleva tiempo; para algunas organizaciones, entre dos y siete minutos.[6] Además, esto hace que los agentes del contact center se sientan interrogadores y temen las consecuencias de no detectar a un delincuente.

El resultado es un tiempo medio de gestión (TMO) largo y agentes ansiosos e insatisfechos. Y, como puede imaginar, es lo último que quiere ver cualquier persona encargada de gestionar un contact center de forma efectiva y productiva.

La duración de cada conversación con el cliente reduce la eficiencia del agente y aumenta los costes de personal. Al mismo tiempo, la baja moral de los agentes aumenta su rotación. Además de los costes adicionales de adquisición de agentes para su contact center, esto conduce a una plantilla de agentes con menos experiencia, lo cual también afecta a la experiencia del cliente.

La digitalización de los servicios, ha provocado un aumento de las interacciones con el cliente en los canales digitales y los responsables del contact center necesitan una forma más eficiente de verificar la identidad de los clientes en estos canales. El 65% de los responsables de la prevención del fraude dicen que los ataques de fraude en los canales digitales están generando costes adicionales en el contact center, debido a la presión y el volumen de incidencias acumuladas pendientes de resolver.[7]

El perjuicio económico para su negocio (un gran motivo para poner solución juntos)

Por lo tanto, para resumir, un proceso de autenticación problemático contribuye a tener:

— Costes por quejas del cliente

— Costes de adquisición de clientes

— Costes de prevención del fraude

— Pérdidas por fraude (y daño reputacional)

— Costes operativos del contact center

— Costes de adquisición de agentes

En pocas palabras, es enormemente costoso para su empresa en general.

Pero ahora vienen las buenas noticias: como responsable de la experiencia del cliente, está en una posición perfecta para liderar el cambio e impulsar los beneficios que se percibirán en toda su organización.

26%

Las empresas que mantienen la rotación de agentes en <15% ven una mejora del 26% en las calificaciones de los clientes.[8]

6 Plazo basado en conversaciones con clientes de Nuance.
7 Informe Tendencias del mercado en la atenuación del fraude digital, Aitë Group.
8 Estudio Nemertes realizado en abril de 2020.

Por qué hay tantas empresas interesadas en la autenticación biométrica

El problema fundamental de los procesos tradicionales de autenticación es fácil de entender: identifican a las personas basándose en lo que saben o en lo que tienen, en lugar de basarse en quiénes son en realidad.

La autenticación biométrica resuelve este problema de inmediato. Utiliza las características físicas y de comportamiento únicas de sus clientes: sus huellas dactilares, su rostro, su voz, la forma en que sostienen el dispositivo, la forma en que escriben, etc., para verificar su identidad.

La biometría de voz, con su facilidad de uso y su grado extremadamente alto de precisión, es una solución cada vez más popular entre las principales empresas de servicios financieros.

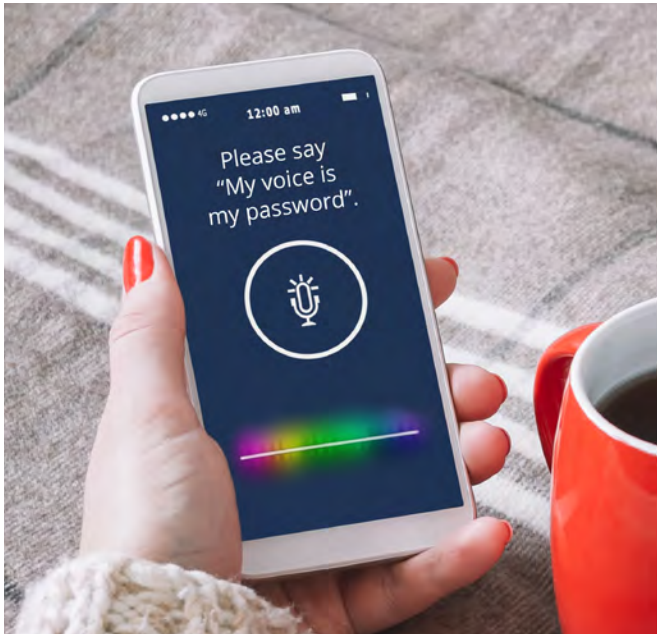
Una vez que un cliente ha generado su "huella de voz", se puede verificar su identidad de forma automática en apenas unos segundos, ya sea en una conversación con un agente, a través de una IVR o en una aplicación del teléfono móvil. El cliente no tiene que recordar una contraseña ni solicitar un código PIN. El agente no tiene que desempeñar el papel de interrogador. Ambos pueden centrarse en resolver la consulta.

Y aún mejor, puede utilizar la biometría de voz para identificar de forma proactiva a delincuentes, comparando su voz con una lista de seguimiento de huellas de voces de estafadores recurrentes.

Así como un proceso de autenticación débil y lento causa problemas en toda la empresa, la velocidad y la seguridad de la biometría de voz pueden generar innumerables beneficios en su empresa.

El 81 %

de los consumidores ven la biometría como una forma más segura de verificación de la identidad.[9]



9 Entrevista con el responsable de innovación de producción de identificación y fraude global en Experian, febrero de 2020.

Los beneficios para usted: una experiencia de cliente de nivel superior

Las soluciones de autenticación por voz pueden ser "activas" o "pasivas". Si son activas, se le pide al cliente que diga una frase fija, a modo de contraseña, para verificar su identidad. Si son pasivas, la autenticación se produce a lo largo de la conversación con una IVR o un agente, verificando la identidad del cliente de forma totalmente natural y sin interrupciones. De cualquier forma, es una experiencia rápida, fácil y segura.

La autenticación por voz le permite atender un mayor volumen de llamadas en la IVR, acortando los tiempos de espera de los clientes y el tiempo que sus agenten tardan en resolver sus consultas. Es fácil, es seguro, reduce costes, y fideliza clientes. ¿Podemos pedir más?

Y si, la biometría de voz tiene sentido más allá del contact center y el canal telefónico. Su uso cada vez más extendido en los canales digitales, permite reforzar la seguridad de las transacciones a través de su app móvil o página web, solicitando al cliente que verifique su identidad desde la propia app para poder realizar una transferencia o cualquier otro tipo de transacción. Reforzar los procesos de autenticación de clientes con biometría es el paso a seguir para proporcionar las experiencias que sus clientes desean mantener con su empresa cumpliendo con los máximos estándares de seguridad.

Mejores experiencias con biometría de voz en Barclays

- Aumento de la satisfacción del cliente y del agente
- El 93% de los clientes puntuaron 9 o 10 (sobre 10) el sistema de identificación y verificación biométrico
- 90% de reducción de las reclamaciones

CSAT & ASAT

"Incorporar la tecnología de biometría de voz de Nuance ha sido fundamental en nuestra misión de ofrecer una experiencia de cliente excelente. Los resultados de satisfacción de clientes y empleados hablan por sí solos. Estamos deseando trabajar con Nuance en el futuro para utilizar la biometría de voz en más canales para autenticar aún más procesos."

— Anne Grim
Directora Global de Experiencia de Cliente
Barclays Wealth and Investment Management

Los beneficios para su contact center: TMO inferior, agentes más felices

Una autenticación más rápida y consistente no solo supone una ventaja para sus clientes: también es una ventaja para su contact center.

En comparación con los métodos de autenticación basados en el conocimiento, las soluciones de autenticación mediante biometría de voz reducen el TMO (Tiempo Medio de Operación) en un promedio de 53 segundos[10] y, a menudo, incluso más. Dado que el éxito de la autenticación ya no depende de la memoria de sus clientes, hay un porcentaje de clientes mucho menor que fallan en la autenticación y se dedica menos tiempo a gestionar estos casos.

Este aumento de la eficiencia del contact center viene acompañado de una reducción en la rotación de los agentes.

Como hemos visto, la autenticación por voz reduce la carga de los agentes que ya no tienen que perder el tiempo bombardeando a los clientes con multitud de preguntas para verificar su identidad, ni aguantar las críticas de los clientes.

Esto les permite concentrarse en ayudar realmente al cliente, lo que aumenta la satisfacción laboral del agente y reduce la probabilidad de que éste abandone su puesto. Esto implica una menor inversión de tiempo y dinero en contratar y formar a nuevos agentes.

Y cuando llega el momento de contratar a un nuevo agente, es más rápido y más fácil que nunca formarlo para llevar a cabo las tareas de identificación, que le permitirá resolver las consultas de los clientes con agilidad.

Reducir el TMO en todo el mundo con biometría de voz

Cliente de biometría de voz de Nuance	Reducción del TMO reportada
Australian Tax Office	48 segundos
Banco Santander	42 segundos
Eastern Bank	60 segundos
Royal Bank of Canada	43 segundos

10 Reducción promedio del AHT calculada basándose en los resultados notificados por los clientes de Nuance.

Prevención del fraude con biometría de voz en NatWest Group

17 millones

de llamadas protegidas al año

+2.500

llamadas fraudulentas detectadas

>300%

ROI durante el primer año

Los beneficios para su equipo de prevención de fraude: reducción de pérdidas y prevención activa

Los sistemas de autenticación biométrica hacen que los delincuentes ya no puedan utilizar nombres de usuario ni contraseñas robadas para cometer una estafa, y son capaces de detectar las técnicas de ingeniería social y notificar sobre lo ocurrido a sus agentes y expertos en prevención de fraude.

Si a esto le sumamos la capacidad de la tecnología para identificar a los estafadores recurrentes, y señalar las llamadas, intentos de acceso y otro tipo de movimientos sospechosos, este tipo de soluciones tendrán un gran impacto en la reducción de las pérdidas y los costes asociados a la prevención del fraude.

La solución de biometría de voz de HSBC en Reino Unido (Voice ID) ha evitado intentos de fraude por valor de 608 millones de libras en menos de dos años. El banco tiene ahora más de tres millones de clientes del Reino Unido registrados en su sistema, que realiza alrededor de nueve millones de verificaciones cada año.[11, 12]

11 https://www.about.hsbc.co.uk/news-and-media/hsbc-voiceid-attempted-fraud (Consultado el 8 de febrero de 2021).
12 https://www.about.hsbc.co.uk/news-and-media/hsbc-uk-launches-new-voice-driven-technology (Consultado el 24 de marzo de 2021).

"El ROI de la herramienta probablemente supere el 300%, por lo que, como recuperación de la inversión de una implementación de tecnología, ha sido impresionante".

— Jason Costain
Director de estrategia contra el fraude y gestión de relaciones NatWest Group (antiguamente Royal Bank of Scotland Group)

El impacto positivo en la reputación para toda su empresa

La introducción de la autenticación por voz, o cualquier otra innovación que mejore sus capacidades de detección y prevención del fraude, refuerza la reputación de su institución financiera, lo que indica claramente el compromiso de su marca con la seguridad y protección de sus clientes.

Al mismo tiempo, le ayuda a protegerse contra el daño reputacional que puede provenir de ataques delictivos de éxito.

El 88%

de los consumidores dice que su percepción de una empresa mejora cuando esta invierte en la experiencia del cliente, es decir, en seguridad.[13]

13 Informe de fraude e identidad global de Experian 2020.

Es el momento de rediseñar su estrategia de identificación y verificación de clientes y sus procesos de autenticación.

Juntos.

Cuando la autenticación es problemática para sus clientes y agentes, es problemática para su empresa. La biometría de voz puede ayudar, especialmente cuando se integra en una solución multi factor que proporciona una vista unificada de la autenticación (y los intentos de fraude) en todos los canales de interacción.

Como responsable de la experiencia, servicio o atención al cliente, está en una posición ideal para reunir a sus colegas del departamento de prevención de fraude y su equipo del contact center para iniciar una transformación que, en última instancia, los ayudará a todos a alcanzar sus objetivos.

Pero no tiene que hacerlo solo: Nuance está aquí para ayudarle, al igual que hemos ayudado a muchas otras empresas de servicios financieros.

MÁS INFORMACIÓN

Obtenga más información sobre las soluciones de prevención del fraude y autenticación biométrica de Nuance en nuestro sitio web.

Descubrirá por qué Opus Research nos nombró "líder indiscutible del mercado" en su conocido reporte anual Intelligent Authentication and Voice Biometrics Intelliview de 2020.

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.

© 2021 Nuance. Todos los derechos reservados.
ENT_4323_01_EB_SP, 6 Sept 2021